

# Exhibit A

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND**  
*Southern Division*

**IN RE: MARRIOTT INTERNATIONAL  
INC., CUSTOMER DATA SECURITY  
BREACH LITIGATION**

MDL No. 19-md-2879

Judge Paul W. Grimm

**THIS DOCUMENT RELATES TO  
THE CONSUMER ACTIONS**

**JURY TRIAL DEMANDED**

**SECOND AMENDED CONSOLIDATED CONSUMER CLASS ACTION  
COMPLAINT**

## **TABLE OF CONTENTS**

<b>INTRODUCTION</b>	1
<b>JURISDICTION AND VENUE</b>	2
<b>DEFENDANTS</b>	4
<b>DEFINITIONS</b>	4
<b>NAMED PLAINTIFFS</b>	5
Alabama	5
Alaska	6
Arizona	7
Arkansas	7
California	8
Colorado	9
Connecticut	10
Delaware	10
Florida	11
Georgia	12
Hawaii	13
Idaho	13
Illinois	14
Indiana	15
Iowa	15
Kansas	15
Kentucky	16
Louisiana	16
Maine	17
Maryland	17
Massachusetts	18
Michigan	18
Minnesota	19
Mississippi	19

Missouri .....	20
Montana .....	21
Nebraska .....	21
Nevada .....	21
New Hampshire .....	22
New Jersey .....	22
New Mexico.....	23
New York.....	23
North Carolina .....	25
North Dakota.....	25
Ohio.....	25
Oklahoma .....	26
Oregon.....	26
Pennsylvania .....	27
Rhode Island .....	27
South Carolina .....	28
South Dakota.....	28
Tennessee.....	28
Texas .....	29
Utah.....	30
Vermont .....	30
Virginia .....	31
Washington .....	31
West Virginia.....	32
Wisconsin.....	32
Wyoming.....	32
<b>FACTUAL ALLEGATIONS.....</b>	<b>33</b>
Marriott International and its Privacy Policy.....	33
Starwood Hotels and Its Preferred Guest Program .....	36
Marriott’s Acquisition of Starwood.....	40
Marriott and Starwood Knew they were Targets of Cyber Threats.....	47
The Data Breach .....	56

Marriott’s Response to the Breach.....	64
Reactions to the Breach and Government and Regulatory Investigations.....	69
An Independent Report Confirms Marriott’s Deficient Data Security Practices .....	74
Accenture’s Role in the Data Breach.....	79
Marriott Failed to Comply with Regulatory Guidance .....	83
The Effect of the Data Breach on Impacted Consumers.....	85
<b>CLASS ACTION ALLEGATIONS .....</b>	<b>91</b>
<b>NATIONWIDE CLASS.....</b>	<b>91</b>
<b>STATEWIDE [NAME OF STATE OR TERRITORY] SUBCLASS.....</b>	<b>91</b>
<b>CHOICE OF LAW FOR NATIONWIDE CLAIMS.....</b>	<b>95</b>
<b>CLAIMS ON BEHALF OF THE NATIONWIDE CLASS AGAINST MARRIOTT AND STARWOOD .....</b>	<b>97</b>
<u>COUNT 1</u> .....	97
NEGLIGENCE	
<u>COUNT 2</u> .....	100
NEGLIGENCE PER SE	
<u>COUNT 3</u> .....	101
BREACH OF CONTRACT	
<u>COUNT 4</u> .....	105
BREACH OF IMPLIED CONTRACT	
<u>COUNT 5</u> .....	106
UNJUST ENRICHMENT	
<u>COUNT 6</u> .....	108
DECLARATORY JUDGMENT	
<u>COUNT 7</u> .....	110
MARYLAND PERSONAL INFORMATION PROTECTION ACT	
Md. Comm. Code §§ 14-3501, et seq.	
<u>COUNT 8</u> .....	112
MARYLAND CONSUMER PROTECTION ACT	
Md. Code Ann., Com. Law §§ 13-301, et seq.	
<b>CLAIMS ON BEHALF OF THE ALABAMA SUBCLASS.....</b>	<b>116</b>

<u>COUNT 9</u> .....	116
ALABAMA DECEPTIVE TRADE PRACTICES ACT	
Ala. Code §§ 8-19-1, et seq.	
<b>CLAIMS ON BEHALF OF THE ALASKA SUBCLASS</b> .....	120
<u>COUNT 10</u> .....	120
PERSONAL INFORMATION PROTECTION ACT	
Alaska Stat. §§ 45.48.010, et seq.	
<u>COUNT 11</u> .....	121
ALASKA CONSUMER PROTECTION ACT	
Alaska Stat. §§ 45.50.471, et seq.	
<b>CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS</b> .....	124
<u>COUNT 12</u> .....	124
ARIZONA CONSUMER FRAUD ACT	
A.R.S. §§ 44-1521, et seq.	
<b>CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS</b> .....	127
<u>COUNT 13</u> .....	127
ARKANSAS DECEPTIVE TRADE PRACTICES ACT	
A.C.A. §§ 4-88-101, et seq.	
<b>CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS</b> .....	131
<u>COUNT 14</u> .....	131
CALIFORNIA CUSTOMER RECORDS ACT	
Cal. Civ. Code §§ 1798.80, et seq.	
<u>COUNT 15</u> .....	133
CALIFORNIA UNFAIR COMPETITION LAW	
Cal. Bus. & Prof. Code §§ 17200, et seq.	
<u>COUNT 16</u> .....	137
CALIFORNIA CONSUMER LEGAL REMEDIES ACT	
Cal. Civ. Code §§ 1750, et seq.	
<b>CLAIMS ON BEHALF OF THE COLORADO SUBCLASS</b> .....	139
<u>COUNT 17</u> .....	139
COLORADO SECURITY BREACH NOTIFICATION ACT	
Colo. Rev. Stat. §§ 6-1-716, et seq.	

<u>COUNT 18</u> .....	140
COLORADO CONSUMER PROTECTION ACT	
Colo. Rev. Stat. §§ 6-1-101, et seq.	
<b>CLAIMS ON BEHALF OF THE CONNECTICUT SUBCLASS</b> .....	143
<u>COUNT 19</u> .....	143
CONNECTICUT UNFAIR TRADE PRACTICES ACT	
C.G.S.A. § 42-110G	
<b>CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS</b> .....	147
<u>COUNT 20</u> .....	147
DELAWARE COMPUTER SECURITY BREACH ACT	
6 Del. Code Ann. §§ 12B-102, et seq.	
<u>COUNT 21</u> .....	148
DELAWARE CONSUMER FRAUD ACT	
6 Del. Code §§ 2513, et seq.	
<b>CLAIMS ON BEHALF OF THE DISTRICT OF COLUMBIA SUBCLASS</b> .....	151
<u>COUNT 22</u> .....	151
DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT	
D.C. Code §§ 28-3851, et seq.	
<u>COUNT 23</u> .....	152
DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT	
D.C. Code §§ 28-3904, et seq.	
<b>CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS</b> .....	155
<u>COUNT 24</u> .....	155
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT	
Fla. Stat. §§ 501.201, et seq.	
<b>CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS</b> .....	158
<u>COUNT 25</u> .....	158
GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT	
Ga. Code Ann. §§ 10-1-370, et seq.	
<u>COUNT 26</u> .....	161
RECOVERY OF EXPENSES OF LITIGATION ON BEHALF OF GEORGIA SUBCLASS	
O.C.G.A. § 13-6-11	

<b>CLAIMS ON BEHALF OF THE HAWAII SUBCLASS .....</b>	<b>162</b>
<u>COUNT 27</u> .....	162
HAWAII SECURITY BREACH NOTIFICATION ACT	
Haw. Rev. Stat. §§ 487N-1, et seq.	
<u>COUNT 28</u> .....	163
HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT	
Haw. Rev. Stat. §§ 480-1, et seq.	
<u>COUNT 29</u> .....	166
HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT	
Haw. Rev. Stat. §§ 481A-3, et seq.	
<b>CLAIMS ON BEHALF OF THE IDAHO SUBCLASS .....</b>	<b>168</b>
<u>COUNT 30</u> .....	168
IDAHO CONSUMER PROTECTION ACT	
Idaho Code §§ 48-601, et seq.	
<b>CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS .....</b>	<b>171</b>
<u>COUNT 31</u> .....	171
ILLINOIS PERSONAL INFORMATION PROTECTION ACT	
815 Ill. Comp. Stat. §§ 530/10(a), et seq.	
<u>COUNT 32</u> .....	172
ILLINOIS CONSUMER FRAUD ACT	
815 Ill. Comp. Stat. §§ 505, et seq.	
<u>COUNT 33</u> .....	175
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT	
815 Ill. Comp. Stat. §§ 510/2, et seq.	
<b>CLAIMS ON BEHALF OF THE INDIANA SUBCLASS .....</b>	<b>178</b>
<u>COUNT 34</u> .....	178
Indiana Deceptive Consumer sales ACT	
Ind. Code §§ 24-5-0.5-1, et seq.	
<b>CLAIMS ON BEHALF OF THE IOWA SUBCLASS .....</b>	<b>184</b>
<u>COUNT 35</u> .....	184
PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW	
Iowa Code § 715C.2	

COUNT 36 .....	185
IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT	
Iowa Code § 714H	
<b>CLAIMS ON BEHALF OF THE KANSAS SUBCLASS .....</b>	<b>187</b>
COUNT 37 .....	187
PROTECTION OF CONSUMER INFORMATION	
Kan. Stat. Ann. §§ 50-7a02(a), et seq.	
COUNT 38 .....	188
KANSAS CONSUMER PROTECTION ACT	
K.S.A. §§ 50-623, et seq.	
<b>CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS .....</b>	<b>192</b>
COUNT 39 .....	192
KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT	
Ky. Rev. Stat. Ann. §§ 365.732, et seq.	
COUNT 40 .....	193
KENTUCKY CONSUMER PROTECTION ACT	
Ky. Rev. Stat. §§ 367.110, et seq.	
<b>CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS .....</b>	<b>196</b>
COUNT 41 .....	196
DATABASE SECURITY BREACH NOTIFICATION LAW	
La. Rev. Stat. Ann. §§ 51:3074(A), et seq.	
COUNT 42 .....	197
LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW	
La Rev. Stat. Ann. §§ 51:1401, et seq.	
<b>CLAIMS ON BEHALF OF THE MAINE SUBCLASS .....</b>	<b>201</b>
COUNT 43 .....	201
MAINE UNFAIR TRADE PRACTICES ACT	
5 Me. Rev. Stat. §§ 205, 213, et seq.	
COUNT 44 .....	203
MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT	
10 Me. Rev. Stat. §§ 1212, et seq.	

<b>CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS .....</b>	<b>206</b>
<u>COUNT 45 .....</u>	<u>206</u>
MASSACHUSETTS CONSUMER PROTECTION ACT	
Mass. Gen. Laws Ann. Ch. 93A, §§ 1, et seq.	
<b>CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS.....</b>	<b>210</b>
<u>COUNT 46 .....</u>	<u>210</u>
MICHIGAN IDENTITY THEFT PROTECTION ACT	
Mich. Comp. Laws Ann. §§ 445.72, et seq.	
<u>COUNT 47 .....</u>	<u>211</u>
MICHIGAN CONSUMER PROTECTION ACT	
Mich. Comp. Laws Ann. §§ 445.903, et seq.	
<b>CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS.....</b>	<b>214</b>
<u>COUNT 48 .....</u>	<u>214</u>
MINNESOTA CONSUMER FRAUD ACT	
Minn. Stat. §§ 325F.68, et seq. and Minn. Stat. §§ 8.31, et seq.	
<u>COUNT 49 .....</u>	<u>217</u>
MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT	
Minn. Stat. §§ 325D.43, et seq.	
<b>CLAIMS ON BEHALF OF THE MISSISSIPPI SUBCLASS.....</b>	<b>220</b>
<u>COUNT 50 .....</u>	<u>220</u>
MISSISSIPPI CONSUMER PROTECTION ACT	
Miss. Code §§ 75-24-1, et seq.	
<b>CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS .....</b>	<b>224</b>
<u>COUNT 51 .....</u>	<u>224</u>
MISSOURI MERCHANDISING PRACTICES ACT	
Mo. Rev. Stat. §§ 407.010, et seq.	
<b>CLAIMS ON BEHALF OF THE MONTANA SUBCLASS .....</b>	<b>226</b>
<u>COUNT 52 .....</u>	<u>226</u>
COMPUTER SECURITY BREACH LAW	
Mont. Code Ann. §§ 30-14-1704(1), et seq.	
<u>COUNT 53 .....</u>	<u>228</u>
MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT	
M.C.A. §§ 30-14-101, et seq.	

<b>CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS .....</b>	<b>231</b>
<u>COUNT 54</u> .....	231
NEBRASKA CONSUMER PROTECTION ACT	
Neb. Rev. Stat. §§ 59-1601, et seq.	
<u>COUNT 55</u> .....	233
NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT	
Neb. Rev. Stat. §§ 87-301, et seq.	
<b>CLAIMS ON BEHALF OF THE NEVADA SUBCLASS .....</b>	<b>237</b>
<u>COUNT 56</u> .....	237
NEVADA DECEPTIVE TRADE PRACTICES ACT	
Nev. Rev. Stat. Ann. §§ 598.0903 et seq.	
<b>CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS .....</b>	<b>240</b>
<u>COUNT 57</u> .....	240
NOTICE OF SECURITY BREACH	
N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), et seq.	
<u>COUNT 58</u> .....	241
NEW HAMPSHIRE CONSUMER PROTECTION ACT	
N.H.R.S.A. §§ 358-A, et seq.	
<b>CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS .....</b>	<b>244</b>
<u>COUNT 59</u> .....	244
NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT	
N.J. Stat. Ann. §§ 56:8-163, et seq.	
<u>COUNT 60</u> .....	245
NEW JERSEY CONSUMER FRAUD ACT	
N.J. Stat. Ann. §§ 56:8-1, et seq.	
<b>CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS .....</b>	<b>248</b>
<u>COUNT 61</u> .....	248
NEW MEXICO UNFAIR PRACTICES ACT	
N.M. Stat. Ann. §§ 57-12-2, et seq.	
<b>CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS.....</b>	<b>251</b>
<u>COUNT 62</u> .....	251
NEW YORK GENERAL BUSINESS LAW	
N.Y. Gen. Bus. Law §§ 349, et seq.	

<b>CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS .....</b>	<b>254</b>
<u>COUNT 63</u> .....	254
NORTH CAROLINA IDENTITY THEFT PROTECTION ACT	
N.C. Gen. Stat. §§ 75-60, et seq.	
<u>COUNT 64</u> .....	255
NORTH CAROLINA UNFAIR TRADE PRACTICES ACT	
N.C. Gen. Stat. Ann. §§ 75-1.1, et seq.	
<b>CLAIMS ON BEHALF OF THE NORTH DAKOTA SUBCLASS .....</b>	<b>258</b>
<u>COUNT 65</u> .....	258
NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION,	
N.D. Cent. Code §§ 51-30-02, et seq.	
<u>COUNT 66</u> .....	259
NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT	
N.D. Cent. Code §§ 51-15-01, et seq.	
<b>CLAIMS ON BEHALF OF THE OHIO SUBCLASS .....</b>	<b>262</b>
<u>COUNT 67</u> .....	262
OHIO CONSUMER SALES PRACTICES ACT	
Ohio Rev. Code §§ 1345.01, et seq.	
<u>COUNT 68</u> .....	265
OHIO DECEPTIVE TRADE PRACTICES ACT	
Ohio Rev. Code §§ 4165.01, et seq.	
<b>CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS .....</b>	<b>268</b>
<u>COUNT 69</u> .....	268
OKLAHOMA CONSUMER PROTECTION ACT	
Okla. Stat. Tit. 15, §§ 751, et seq.	
<b>CLAIMS ON BEHALF OF THE OREGON SUBCLASS .....</b>	<b>272</b>
<u>COUNT 70</u> .....	272
OREGON CONSUMER IDENTITY THEFT PROTECTION ACT	
Or. Rev. Stat. §§ 646A.604(1), et seq.	
<u>COUNT 71</u> .....	273
OREGON UNLAWFUL TRADE PRACTICES ACT	
Or. Rev. Stat. §§ 646.608, et seq.	

<b>CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS.....</b>	<b>277</b>
<u>COUNT 72</u> .....	277
PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW 73 Pa. Cons. Stat. §§ 201-2 & 201-3, et seq.	
<b>CLAIMS ON BEHALF OF THE PUERTO RICO SUBCLASS .....</b>	<b>280</b>
<u>COUNT 73</u> .....	280
CITIZEN INFORMATION ON DATA BANKS SECURITY ACT P.R. Laws Ann. tit. 10, §§ 4051, et seq.	
<b>CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS.....</b>	<b>281</b>
<u>COUNT 74</u> .....	281
RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT R.I. Gen. Laws §§ 6-13.1, et seq.	
<b>CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS.....</b>	<b>285</b>
<u>COUNT 75</u> .....	285
SOUTH CAROLINA DATA BREACH SECURITY ACT S.C. Code Ann. §§ 39-1-90, et seq.	
<u>COUNT 76</u> .....	286
SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT S.C. Code Ann. §§ 39-5-10, et seq.	
<b>CLAIMS ON BEHALF OF THE SOUTH DAKOTA SUBCLASS.....</b>	<b>291</b>
<u>COUNT 77</u> .....	291
SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT S.D. Codified Laws §§ 37-24-1, et seq.	
<b>CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS.....</b>	<b>294</b>
<u>COUNT 78</u> .....	294
TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT Tenn. Code Ann. §§ 47-18-2107, et seq.	
<u>COUNT 79</u> .....	295
TENNESSEE CONSUMER PROTECTION ACT Tenn. Code Ann. §§ 47-18-101, et seq.	

<b>CLAIMS ON BEHALF OF THE TEXAS SUBCLASS .....</b>	<b>300</b>
<u>COUNT 80</u> .....	300
DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT	
Texas Bus. & Com. Code §§ 17.41, et seq.	
<b>CLAIMS ON BEHALF OF THE UTAH SUBCLASS .....</b>	<b>306</b>
<u>COUNT 81</u> .....	306
UTAH CONSUMER SALES PRACTICES ACT	
Utah Code §§ 13-11-1, et seq.	
<b>CLAIMS ON BEHALF OF THE VERMONT SUBCLASS .....</b>	<b>311</b>
<u>COUNT 82</u> .....	311
VERMONT CONSUMER FRAUD ACT	
Vt. Stat. Ann. Tit. 9, §§ 2451, et seq.	
<b>CLAIMS ON BEHALF OF THE VIRGIN ISLANDS SUBCLASS .....</b>	<b>315</b>
<u>COUNT 83</u> .....	315
IDENTITY THEFT PREVENTION ACT	
V.I. Code Ann. tit. 14 §§ 2208, et seq.	
<u>COUNT 84</u> .....	315
VIRGIN ISLANDS CONSUMER FRAUD AND DECEPTIVE BUSINESS	
PRACTICES ACT	
Virgin Islands Code tit. 12A, §§ 301, et seq.	
<u>COUNT 85</u> .....	320
VIRGIN ISLANDS CONSUMER PROTECTION LAW	
V.I. Code tit. 12A, §§101, et seq.	
<b>CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS .....</b>	<b>324</b>
<u>COUNT 86</u> .....	324
VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT	
Va. Code. Ann. §§ 18.2-186.6, et seq.	
<u>COUNT 87</u> .....	325
VIRGINIA CONSUMER PROTECTION ACT	
Va. Code Ann. §§ 59.1-196, et seq.	

<b>CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS .....</b>	<b>329</b>
<u>COUNT 88</u> .....	329
WASHINGTON DATA BREACH NOTICE ACT	
Wash. Rev. Code §§ 19.255.010, et seq.	
<u>COUNT 89</u> .....	330
WASHINGTON CONSUMER PROTECTION ACT	
Wash. Rev. Code Ann. §§ 19.86.020, et seq.	
<b>CLAIMS ON BEHALF OF THE WEST VIRGINIA SUBCLASS .....</b>	<b>333</b>
<u>COUNT 90</u> .....	333
WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT	
W. Va. Code §§46A-6-101, et seq.	
<b>CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS .....</b>	<b>339</b>
<u>COUNT 91</u> .....	339
NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION	
Wis. Stat. §§ 134.98(2), et seq.	
<u>COUNT 92</u> .....	340
WISCONSIN DECEPTIVE TRADE PRACTICES ACT	
Wis. Stat. § 100.18	
<b>CLAIMS ON BEHALF OF THE WYOMING SUBCLASS .....</b>	<b>344</b>
<u>COUNT 93</u> .....	344
COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS	
Wyo. Stat. Ann. §§ 40-12-502(a), et seq.	
<u>COUNT 94</u> .....	345
WYOMING CONSUMER PROTECTION ACT	
Wyo. Stat. Ann. §§ 40-12-101, et seq.	
<b>CLAIMS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ACCENTURE .....</b>	<b>350</b>
<u>COUNT 95</u> .....	350
NEGLIGENCE	
<u>COUNT 96</u> .....	353
NEGLIGENCE PER SE	

**REQUEST FOR RELIEF ..... 355**

**DEMAND FOR JURY TRIAL..... 355**

## **INTRODUCTION**

1. On November 30, 2018, Marriott announced that it was subject to one of the largest data breaches in history when the sensitive personal and financial information of up to 500 million hotel guests was exfiltrated from its Starwood guest reservation database as part of an extensive, four-year long data breach.

2. Beginning in July 2014 and continuing through September 2018, hackers exploited glaring vulnerabilities in the Starwood network to install malicious software, harvest user credentials, and roam freely across the Starwood networks to steal valuable consumer data. The stolen information includes names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, payment card numbers, payment card expiration dates, and tools needed to decrypt cardholder data. Perhaps most shockingly, given the extended period during which the hackers had access to Starwood's systems, Marriott has been unable to definitively determine how much data was stolen beyond the limited data it has been able to identify, since several files that the hackers appear to have exfiltrated were deleted.

3. Subsequently, Marriott disclosed that after removing duplicates, the data breach impacted at least 383 million guest records—making it one of the largest data breaches in history. The impacted records Marriott was able to identify include nearly 24 million passport numbers (more than 5 million of which were unencrypted), and more than 9 million credit and debit cards. Marriott has asserted it does not know who carried out the attack.

4. Defendants are responsible for allowing the breach to occur because they failed to implement and maintain any reasonable safeguards and failed to comply with industry-standard

data security practices, contrary to the representations made in Marriott's privacy statements and its explicit and implied agreements with its hotel guests.

5. During the four-year data breach period, one of the longest undiscovered breach periods ever, Marriott (and its third party IT security provider, Accenture) failed to detect the hackers' presence, notice the massive amounts of data that was being exfiltrated from Starwood's databases, and failed to take any steps to investigate the numerous other red flags that should have warned the companies that Starwood's systems were not secure – even in the face of other breaches at Starwood and despite the extensive due diligence Marriott should have undertaken in purchasing Starwood. As a result of Defendants' failure to protect the consumer information they were entrusted to safeguard, Plaintiffs and class members did not receive the benefits of their bargains—protection of their Personal Information when transacting with Marriott—and have been exposed to and/or are at significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiffs and class members have also lost the inherent value of their Personal Information.

### **JURISDICTION AND VENUE**

6. This Consolidated Complaint is intended to serve as a superseding complaint as to all other complaints consolidated in this multidistrict litigation that were filed on behalf of consumers, and to serve for all purposes as the operative pleading for the Classes defined below.

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000.00 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because the majority of putative class members are citizens of a different state than Marriott. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

8. This Court has personal jurisdiction over Marriott because it is headquartered in and maintains its principal place of business in this District. Marriott is authorized to and regularly conducts business in Maryland. In this District, Marriott makes decisions regarding corporate governance and management of the hotels that it owns or manages, including decisions regarding the security measures to protect its customers' Personal Information. Marriott owns and operates many hotels throughout Maryland, the United States, and internationally. Marriott intentionally avails itself of this jurisdiction by promoting, selling and marketing its services from Maryland to millions of consumers nationwide.

9. This Court has personal jurisdiction over Starwood because Starwood is incorporated in Maryland, maintains its principal place of business in Maryland, regularly conducts business in Maryland and has sufficient minimum contacts in Maryland such that Starwood intentionally avails itself of this Court's jurisdiction by conducting corporate operations here and promoting, selling and marketing its services from this District to millions of consumers nationwide.

10. This Court has personal jurisdiction over Accenture because it is authorized to and regularly conducts business in Maryland and has sufficient minimum contacts in Maryland such that Accenture intentionally avails itself of this Court's jurisdiction by conducting operations here and promoting, selling and marketing its services in this District.

11. Venue is proper in this District under 28 U.S.C. 1391(a) through (d) because Marriott's headquarters and principal place of business are located in this District, Starwood resides in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Marriott's governance and management personnel or inaction by those individuals that led to

misrepresentations, invasions of privacy and the Data Breach. Moreover, Accenture maintains an office in this District, conducts business in this District, and provided services to Marriott and Starwood in this District.

### **DEFENDANTS**

12. Defendant Marriott International, Inc. is a Delaware corporation with its principal place of business in Bethesda, Maryland.

13. Defendant Starwood Hotels & Resorts Worldwide, LLC is a Maryland limited liability company with its principal place of business in Bethesda, Maryland. Starwood is now a wholly-owned subsidiary of Defendant Marriott.

14. Defendant Accenture plc is an Irish public limited company, with its principal executive offices in Dublin, Ireland and operates its business through subsidiaries of Accenture plc. Defendant Accenture LLP is a subsidiary of Accenture plc and a limited liability partnership organized under the laws of the state of Illinois. Defendants Accenture plc and Accenture LLP are collectively referred to herein as “Accenture.”

### **DEFINITIONS**

15. As used throughout this Complaint, “Data Breach” refers to the data security incident involving the Starwood guest reservation database announced by Marriott on November 30, 2018.

16. As used throughout this Complaint, “Marriott” is defined to include Marriott International, Inc., Starwood Hotels & Resorts Worldwide, LLC, Starwood Hotels & Resorts Worldwide, Inc., and any other wholly-owned subsidiaries of Marriott International, Inc.

17. As used throughout this Complaint, “Personal Information” is defined to include all information exposed in the Data Breach, including all or any part or combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest

account information, date of birth, gender, arrival and departure information, reservation date, communication preferences, payment card numbers, and payment card expiration dates.

18. As used throughout this Complaint, “Marriott Property” is defined to include any Marriott property collecting guest information that was compromised in the Data Breach including W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels, and Starwood-branded timeshare properties Sheraton Vacation Club, Westin Vacation Club, The Luxury Collection Residence Club, St. Regis Residence Club, and Vistana.

#### **NAMED PLAINTIFFS**

19. Plaintiffs are individuals who provided their Personal Information to Marriott, including payment card information, and upon information and belief, had such information compromised in the Data Breach. Plaintiffs bring this action on behalf of themselves and all those similarly situated both across the United States and within their State or Territory of residence. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because Marriott has exclusive but incomplete knowledge of what information was compromised for each individual, including payment card and passport information, Plaintiffs reserve their right to supplement their allegations with additional facts and injuries as they are discovered.

#### **ALABAMA**

20. Plaintiff Keith Williams is a resident of the State of Alabama and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Williams has suffered identity theft and fraud in the form of unauthorized accounts opened and applied for in his name and unauthorized tax returns filed in

his name. As a result, Plaintiff Williams spent time and money signing up for credit monitoring, freezing his credit, filing a police report, contacting banks and credit card companies, and contacting and filing paperwork with the IRS, the Social Security Administration, and state attorneys general offices to resolve the identity theft and fraud issues. Further, as a result of the Data Breach and an inability to resolve the issues caused by the fraudulently filed tax return, Plaintiff has not received tax refunds owed to him. As a direct result of the Data Breach, Plaintiff Williams spent time and money enrolling in credit monitoring and freezing his credit to mitigate potential harm. Prior to the announcement of the Data Breach, Plaintiff Williams used his debit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Williams subsequently experienced unauthorized charges on this same payment card. As a result of this fraud, Plaintiff Williams spent time investigating the source of the unauthorized charges and working with his bank to reverse the charges and get a new card. In addition, as a result of the Data Breach, Plaintiff Williams spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Williams remains at a substantial and imminent risk of future harm.

### **ALASKA**

21. Plaintiff Teresa Borman is a resident of the State of Alaska and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Borman spent time and effort regularly monitoring her accounts to detect fraudulent activity and monitoring her credit accounts through a credit monitoring service in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Borman remains at a substantial and imminent risk of future harm.

### **ARIZONA**

22. Plaintiff Nathan Esquerra is a resident of the State of Arizona and provided his Personal Information to Marriott in order to purchase a Marriott timeshare and stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Esquerra spent time and money purchasing credit monitoring in order to mitigate against potential harm. In addition, as a result of the Data Breach, Plaintiff Esquerra spent time and effort monitoring his credit score and financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Esquerra remains at a substantial and imminent risk of future harm.

### **ARKANSAS**

23. Plaintiff Sean Phillips is a resident of the State of Arkansas and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Phillips has suffered identity theft and fraud in the form of unauthorized accounts opened in his name, unauthorized debit and credit cards opened and applied for in his name, and unauthorized tax returns filed in his name. As a result of this identity theft and fraud, Plaintiff Phillips spent time filing a police report regarding the fraudulently filed tax return, working with the SEC and IRS to resolve the fraudulent tax return issues, working with his bank to combat fraud on his account and to shut down fraudulently opened debit and credit cards, and working with a retailer to shut down a fraudulently opened account. Further, as a result of the Data Breach and an inability to resolve the issues caused by the fraudulently filed tax returns, Plaintiff Phillips has not received the tax refund owed to him. Plaintiff Phillips has also spent time and effort freezing his credit, monitoring his financial accounts, and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Phillips remains at a substantial and imminent risk of future harm.

24. Plaintiff William Boyd is a resident of the State of Arkansas and provided his Personal Information to Marriott in order to purchase incidentals at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Boyd spent time and effort researching the Data Breach and its impact, and monitoring his financial accounts and credit reports to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Boyd remains at a substantial and imminent risk of future harm.

### **CALIFORNIA**

25. Plaintiff Robert Guzikowski is a resident of the State of California and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Guzikowski also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Guzikowski spent time and money purchasing credit monitoring and identity theft protection services and making international calls in order to mitigate against potential harm. In addition, as a result of the Data Breach, Plaintiff Guzikowski spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Guzikowski remains at a substantial and imminent risk of future harm.

26. Plaintiff Denitric Marks is a resident of the State of California and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Marks spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Marks remains at a substantial and imminent risk of future harm.

27. Plaintiff Janel Sempre is a resident of the State of California and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Sempre spent time and money purchasing credit

monitoring and identity theft protection services and reviewing her credit reports to detect fraudulent activity. Plaintiff Sempre also spent time and effort monitoring her financial accounts to detect fraudulent activity, researching the Data Breach, and calling her bank and credit card companies to ensure her accounts were secure. Given the highly-sensitive nature of the information stolen, Plaintiff Sempre remains at a substantial and imminent risk of future harm.

28. Plaintiff Maria Maisto is a resident of the State of California and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Maisto also provided her passport information in order to stay at a Marriott Property. Prior to the announcement of the Data Breach, Plaintiff Maisto used her credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Maisto spent time and effort monitoring her financial accounts and credit card statements to detect fraudulent activity and uses a credit monitoring service in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Maisto remains at a substantial and imminent risk of future harm.

### **COLORADO**

29. Plaintiff Matthew Crabtree is a resident of the State of Colorado and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Crabtree also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Crabtree spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Crabtree remains at a substantial and imminent risk of future harm.

30. Plaintiff Travis Bowlby is a resident of the State of Colorado and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Prior to the announcement of the Data Breach, Plaintiff Bowlby used his credit card to purchase

goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Bowlby suffered identity theft and fraud in the form of several unauthorized accounts being applied for in his name. As a result of this identity theft and fraud, Plaintiff Bowlby spent time and money speaking over the phone with creditors and credit report officials, investigating and monitoring his credit for additional fraudulent activity, filling out paperwork, and paying for postage to correspond with creditors. In addition, as a result of the Data Breach, Plaintiff Bowlby spent time and money setting up credit freezes to help mitigate against potential harm. Given the highly sensitive nature of the information stolen, Plaintiff Bowlby remains at a substantial and imminent risk of future harm.

31. Plaintiff Joan Knudson is a resident of the State of Colorado and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Knudson spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Knudson remains at a substantial and imminent risk of future harm.

### **CONNECTICUT**

32. Plaintiff Anne Marie Amarena is a resident of the State of Connecticut and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Amarena also provided her passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Amarena spent time calling her credit card company, filling out forms, checking her credit report and monitoring her accounts to detect fraudulent charges. Given the highly-sensitive nature of the information stolen, Plaintiff Amarena remains at a substantial and imminent risk of future harm.

### **DELAWARE**

33. Plaintiff Frank Ragan is a resident of the State of Delaware and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach.

As a result of the Data Breach, Plaintiff Ragan spent time and effort contacting his bank to mitigate against potential harm and updating various accounts in order to keep them secure. In addition, as a result of the Data Breach, Plaintiff Ragan spent time and effort monitoring his financial accounts, credit reports, and credit card statements for suspicious and fraudulent activity and to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Ragan remains at a substantial and imminent risk of future harm.

### **FLORIDA**

34. Plaintiff Irma Lawrence is a resident of the State of Florida and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Lawrence also provided her passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Lawrence spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Lawrence remains at a substantial and imminent risk of future harm.

35. Plaintiff Michaela Bittner is a resident of the State of Florida and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Prior to the announcement of the Data Breach, Plaintiff Bittner used her credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Bittner spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly sensitive nature of the information stolen, Plaintiff Bittner remains at a substantial and imminent risk of future harm.

36. Plaintiff Kathleen Frakes Hevener is a resident of the State of Florida and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Subsequent to the Data Breach, Plaintiff Hevener suffered identity theft and fraud in the form of unauthorized credit cards applied for in her name. As a result of this identity theft and fraud,

Plaintiff Hevener spent time and effort contacting banks and credit reporting agencies to cancel these fraudulent accounts and remove them from her credit report. Plaintiff Hevener also spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly sensitive nature of the information stolen, Plaintiff Hevener remains at a substantial and imminent risk of future harm.

### **GEORGIA**

37. Plaintiff Brent Long is a resident of the State of Georgia and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Long also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Long has spent time and money enrolling in credit monitoring and identity theft protection services in order to mitigate against potential harm. In addition, as a result of the Data Breach, Plaintiff Long spent time and effort monitoring financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Long remains at a substantial and imminent risk of future harm.

38. Plaintiff David Viggiano is a resident of the State of Georgia and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Viggiano also provided his passport information in order to stay at a Marriott Property. As a result of the breach, Plaintiff Viggiano spent time and money replacing his passport in order to mitigate against potential harm. In addition, as a result of the Data Breach, Plaintiff Viggiano spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Viggiano remains at a substantial and imminent risk of future harm.

39. Plaintiff Mary Ann Miller is a resident of the State of Georgia and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach.

Prior to the announcement of the Data Breach, Plaintiff Miller used her credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Miller spent time and effort monitoring her financial accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Miller remains at a substantial and imminent risk of future harm.

### **HAWAII**

40. Plaintiff Michael Podesta is a resident of the State of Hawaii and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Prior to the announcement of the Data Breach, Plaintiff Podesta used his credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Podesta subsequently experienced unauthorized charges on this same payment card. As a result of this fraud, Plaintiff Podesta spent time and effort contacting his credit card company to have the unauthorized charges reversed and a new card issued. Plaintiff Podesta also spent time and effort researching the Data Breach, monitoring his financial accounts to detect fraudulent activity, and enrolling in credit monitoring services in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Podesta remains at a substantial and imminent risk of future harm.

### **IDAHO**

41. Plaintiff William Muckelroy II is a resident of the State of Idaho and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Muckelroy II also provided his passport information when staying at a Marriott Property. After learning his passport information may have been compromised, Plaintiff Muckelroy II spent time and money purchasing a replacement passport in order to mitigate against potential harm. Prior to the announcement of the Data Breach, Plaintiff Muckelroy II used his credit card to

purchase goods or services at a Marriott Property. In addition, as a result of the Data Breach, Plaintiff Muckelroy II spent time and effort enrolling in credit monitoring services and monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Muckelroy II remains at a substantial and imminent risk of future harm.

### **ILLINOIS**

42. Plaintiff Barry Golin is a resident of the State of Illinois and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Golin also provided his passport information in order to stay at a Marriott Property. Prior to the announcement of the Data Breach, Plaintiff Golin used his credit card to purchase goods or services at Marriott Properties. As a result of the Data Breach, Plaintiff Golin experienced unauthorized charges on this same payment card. As a result of this fraud, Plaintiff Golin spent time speaking with the police and the FBI, and working with his credit card companies to get the unauthorized charges reversed. Given the highly-sensitive nature of the information stolen, Plaintiff Golin remains at a substantial and imminent risk of future harm.

43. Plaintiff Susan Raab is a resident of the State of Illinois and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Raab also provided her passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Raab spent time reviewing her statements and contacting her credit card companies to detect fraudulent activity and mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Raab remains at a substantial and imminent risk of future harm.

### **INDIANA**

44. Plaintiff Leslie Dallner is a resident of the State of Indiana and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Dallner has suffered identity theft and fraud in the form of unauthorized accounts opened in her name and fraudulent checks cashed in her name. Plaintiff Dallner spent time and effort monitoring her financial accounts to detect fraudulent activity, cancelling the credit cards she used at Marriott, changing her bank account information, engaging in credit monitoring, and taking other steps to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Dallner remains at a substantial and imminent risk of future harm.

### **IOWA**

45. Plaintiff Sherita Olive-Miller is a resident of the State of Iowa and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Olive-Miller spent time and money monitoring her financial accounts to detect fraudulent activity, addressing suspicious activity, closing several credit card accounts used at Marriott, enrolling in credit monitoring services, securing credit freezes, and taking other steps to help mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Olive-Miller remains at a substantial and imminent risk of future harm.

### **KANSAS**

46. Plaintiff Mary Jo Jurey is a resident of the State of Kansas and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Jurey spent time and effort monitoring her financial accounts to detect fraudulent activity and monitoring her credit accounts through a credit

monitoring service in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Jurey remains at a substantial and imminent risk of future harm.

### **KENTUCKY**

47. Plaintiff Timothy Hawkins is a resident of the State of Kentucky and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Hawkins spent time and effort monitoring financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Hawkins remains at a substantial and imminent risk of future harm.

### **LOUISIANA**

48. Plaintiff Anastasia McGee is a resident of the State of Louisiana and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff McGee has suffered identity theft and fraud in the form of an unauthorized party opening a Bitcoin account using her Personal Information. As a result of this fraud, Plaintiff McGee has spent significant time and effort attempting to resolve the issue and close the account. Plaintiff McGee also spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff McGee remains at a substantial and imminent risk of future harm.

49. Plaintiff Lisa Henderson is a resident of the State of Louisiana and provided her Personal Information to Marriott in order to participate in the Marriott program prior to the Data Breach. As a result of the Data Breach, Plaintiff Henderson spent time and effort reviewing her credit card statements and monitoring credit reports to detect suspicious and fraudulent activity. Given the highly sensitive nature of the information stolen, Plaintiff Henderson remains at a substantial and imminent risk of future harm.

**MAINE**

50. Plaintiff Sheila Coughlin is a resident of the State of Maine and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Coughlin also provided her passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Coughlin spent time and money replacing her passport in order to mitigate against potential harm. In addition, as a result of the Data Breach, Plaintiff Coughlin spent time and effort monitoring her financial accounts, credit reports, and credit card statements to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Coughlin remains at a substantial and imminent risk of future harm.

51. Plaintiff Bruce Fitzgerald is a resident of the State of Maine and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Fitzgerald also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Fitzgerald suffered from identity theft and fraud in the form of unauthorized parties opening of fraudulent accounts in his name. As a result of this identity theft and fraud, Plaintiff Fitzgerald spent time and effort reporting these activities to the police, monitoring his accounts to detect fraudulent activity, and contacting the banks where the applications had been submitted to ensure the accounts were closed. Plaintiff Fitzgerald also subsequently paid to have a new passport issued and enrolled in credit monitoring in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Fitzgerald remains at a substantial and imminent risk of future harm.

**MARYLAND**

52. Plaintiff Peter Maldini is a resident of the State of Maryland and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Prior to the announcement of the Data Breach, Plaintiff Maldini used his credit card to purchase

goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Maldini spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Maldini remains at a substantial and imminent risk of future harm.

53. Plaintiff Richard Ryans is a resident of the State of Maryland and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Ryans spent time and effort taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Given the highly-sensitive nature of the information stolen, Plaintiff Ryans remains at a substantial and imminent risk of future harm.

#### **MASSACHUSETTS**

54. Plaintiff Dallas Perkins is a resident of the State of Massachusetts and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Perkins also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Perkins spent time and effort reviewing his financial statements to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Perkins remains at a substantial and imminent risk of future harm.

#### **MICHIGAN**

55. Plaintiff Bryan Wallace is a resident of the State of Michigan and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Wallace spent time and effort contacting his credit card company to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Wallace remains at a substantial and imminent risk of future harm.

56. Plaintiff Laura Gononian is a resident of the State of Michigan and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Gononian also provided her passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Gononian spent time and effort reviewing her account statements and contacting her credit card companies to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Gononian remains at a substantial and imminent risk of future harm.

### **MINNESOTA**

57. Plaintiff Linda Wu is a resident of the State of Minnesota and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Wu also provided her passport information in order to stay at a Marriott Property. Prior to the announcement of the Data Breach, Plaintiff Wu used her credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Wu subsequently experienced unauthorized charges on this same payment card. Plaintiff Wu also spent time and effort reviewing her credit card statements to detect fraudulent activity, changing her account passwords to mitigate against potential harm, and reviewing her credit card monitoring reports, which recently informed her that her email address linked to her SPG membership was the subject of unauthorized activity. Given the highly-sensitive nature of the information stolen, Plaintiff Wu remains at a substantial and imminent risk of future harm.

### **MISSISSIPPI**

58. Plaintiff Shaun Yurtkuran is a resident of the State of Mississippi and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Prior to the announcement of the Data Breach, Plaintiff Yurtkuran used his debit card and credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff

Yurtkuran subsequently experienced unauthorized charges on these same payment cards. As a result of this fraud, Plaintiff Yurtkuran spent time and effort resetting the automatic payment instructions for multiple accounts, contacting and traveling to his bank to address the unauthorized charges, and contacting other merchants with which he does business to update his new card information. In addition, as a result of the Data Breach, Plaintiff Yurtkuran spent time and effort monitoring financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Yurtkuran remains at a substantial and imminent risk of future harm.

### **MISSOURI**

59. Plaintiff Steven Jamison is a resident of the State of Missouri and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Jamison spent time and effort reviewing his financial statements to detect fraudulent activity and contacting his bank to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Jamison remains at a substantial and imminent risk of future harm.

60. Plaintiff Brent McArthur is a resident of the State of Missouri and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff McArthur also provided his passport Information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff McArthur spent time and money monitoring his accounts and purchasing credit monitoring services in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff McArthur remains at a substantial and imminent risk of future harm.

**MONTANA**

61. Plaintiff Holger Meyer is a resident of the State of Montana and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Meyer also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Meyer spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Meyer remains at a substantial and imminent risk of future harm.

**NEBRASKA**

62. Plaintiff Kathleen Christensen is a resident of the State of Nebraska and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Christensen spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Christensen remains at a substantial and imminent risk of future harm.

**NEVADA**

63. Plaintiff Salvatore Caponigro is a resident of the State of Nevada and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Caponigro spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Caponigro remains at a substantial and imminent risk of future harm.

64. Plaintiff Cheryl Pilon Meyer is a resident of the State of Nevada and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Meyer spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly sensitive nature of the information stolen, Plaintiff Meyer remains at a substantial and imminent risk of future harm.

**NEW HAMPSHIRE**

65. Plaintiff Nicole King is a resident of the State of New Hampshire and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff King also provided her passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff King was the victim of a mobile phishing scam that resulted in unauthorized and unreimbursed purchases made using her Personal Information. As a result, Plaintiff King spent time and effort attempting to address the fraud, including filing a police report. In addition, as a result of the Data Breach, Plaintiff King spent time and effort monitoring her financial accounts, credit reports, and credit card statements for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff King remains at a substantial and imminent risk of future harm.

**NEW JERSEY**

66. Plaintiff Svetlana Shtofmakher is a resident of the State of New Jersey and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Shtofmakher spent time and effort monitoring her financial accounts to detect for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Shtofmakher remains at a substantial and imminent risk of future harm.

67. Plaintiff Mary Ann Sundius-Rose is a resident of the State of New Jersey and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Sundius-Rose spent time and effort monitoring her financial accounts to detect fraudulent activity and contacting her bank to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Sundius-Rose remains at a substantial and imminent risk of future harm.

68. Plaintiff Marc Weinberg is a resident of the State of New Jersey and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Prior to the announcement of the Data Breach, Plaintiff Weinberg used his credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Weinberg suffered identity theft and fraud in the form of unauthorized charges. As a result of this identity theft and fraud, Plaintiff Weinberg spent time disputing the charges and attempting to resolve further identity theft and fraud with his credit card companies. Given the highly-sensitive nature of the information stolen, Plaintiff Weinberg remains at a substantial and imminent risk of future harm.

#### **NEW MEXICO**

69. Plaintiff Kris Morris is a resident of the State of New Mexico and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Morris spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Morris remains at a substantial and imminent risk of future harm.

#### **NEW YORK**

70. Plaintiff Roger Cullen is a resident of New York and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Cullen also provided his passport information in order to stay at a Marriott Property. Prior to the announcement of the Data Breach, Plaintiff Cullen used his SPG payment card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Cullen experienced unauthorized charges on this same payment card, as well as unauthorized purchases made from his personal checking account. As a result of this fraud, Plaintiff Cullen spent significant time and effort reviewing charges and speaking on the phone with representatives from his bank in order to replace his card, resolve the fraudulent charges, and mitigate potential harm. In addition, as a result

of the Data Breach, Plaintiff Cullen spent time and effort reviewing his accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Cullen remains at a substantial and imminent risk of future harm.

71. Plaintiff Eric Fishon is a resident of New York and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Fishon spent time and money purchasing credit monitoring, making multiple calls and visits to banks, and time spent contacting Marriott about the Data Breach in order to mitigate against potential harm. In addition, as a result of the Data Breach, Plaintiff Fishon spent significant time monitoring his accounts in order to detect any fraudulent activity and mitigate against potential harm, making phone calls to the bank, reviewing account statements, monitoring credit reports, and communicating with representatives from the credit monitoring service he purchased in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Fishon remains at a substantial and imminent risk of future harm.

72. Plaintiff Paula O'Brien is a resident of New York and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Prior to the announcement of the Data Breach, Plaintiff O'Brien used her credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff O'Brien subsequently experienced unauthorized charges on this same payment card. As a result of this fraud, Plaintiff O'Brien was forced to replace her card, reset automatic payment instructions for multiple accounts, and spend time communicating with her bank to reverse the charges. In addition, as a result of the Data Breach, Plaintiff O'Brien spent time and effort reviewing her account statements in order to

detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff O'Brien remains at a substantial and imminent risk of future harm.

#### **NORTH CAROLINA**

73. Plaintiff Alan Teitleman is a resident of North Carolina and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Teitleman also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Teitleman spent time and effort reviewing his account history, monitoring credit reports, and communicating with Marriott regarding the exposure of his Personal Information. Given the highly-sensitive nature of the information stolen, Plaintiff Teitleman remains at a substantial and imminent risk of future harm.

#### **NORTH DAKOTA**

74. Plaintiff Cleary Johs is a resident of the State of North Dakota and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Johs spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Johs remains at a substantial and imminent risk of future harm.

#### **OHIO**

75. Plaintiff Eric Dubitsky is a resident of the State of Ohio and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Dubitsky spent time and money purchasing identity theft protection services in order to mitigate against potential harm. In addition, as a result of the Data Breach, Plaintiff Dubitsky spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Dubitsky remains at a substantial and imminent risk of future harm.

### **OKLAHOMA**

76. Plaintiff Susan Mullins is a resident of the State of Oklahoma and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Mullins received notice from Marriott by email that her Personal Information was compromised in the Data Breach. As a result of the Data Breach, Plaintiff Mullins spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Mullins remains at a substantial and imminent risk of future harm.

### **OREGON**

77. Plaintiff Adam Ropp is a resident of Oregon and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Ropp also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Ropp suffered identity theft and fraud in the form multiple unauthorized accounts for credit cards, consolidated loans, consumer accounts, and other lines of credit opened using his Personal Information. Plaintiff Ropp is currently working with the IRS in order to resolve his most recent tax refund being collected by an unauthorized individual. As a result, Plaintiff Ropp spent time and money monitoring his accounts and purchasing identity theft insurance in order to mitigate against potential harm. Plaintiff Ropp also invested money in protecting his account information and spent numerous hours reviewing account records, speaking on the phone with representatives from the bank, and sending letters to credit card companies to mitigate against further harm. In addition, as a result of the Data Breach, Plaintiff Ropp spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Ropp remains at a substantial and imminent risk of future harm.

### **PENNSYLVANIA**

78. Plaintiff Fredric Lazarus is a resident of Pennsylvania and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Lazarus also provided his passport information in order to stay at a Marriott Property. Prior to the announcement of the Data Breach, Plaintiff Lazarus used his personal credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Lazarus subsequently experienced unauthorized charges on this same payment card. As a result of this fraud, Plaintiff Lazarus spent multiple hours on calls with his credit card company, obtaining new credit cards and changing the payment information on various accounts and websites. In addition, as a result of the Data Breach, Plaintiff Lazarus spent time and effort monitoring his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Lazarus remains at a substantial and imminent risk of future harm.

79. Plaintiff Robert Reynolds is a resident of Pennsylvania and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Prior to the announcement of the Data Breach, Plaintiff Reynolds used his credit card to purchase goods or services at a Marriott Property. As a result of the Data Breach, Plaintiff Reynolds spent time enrolling in credit monitoring in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Reynolds remains at a substantial and imminent risk of future harm.

### **RHODE ISLAND**

80. Plaintiff Laura Messier is a resident of the State of Rhode Island and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Messier spent time and effort monitoring her financial

accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Messier remains at a substantial and imminent risk of future harm.

### **SOUTH CAROLINA**

81. Plaintiff Josiah Trager is a resident of South Carolina and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Trager spent time and effort monitoring his financial accounts to detect fraudulent activity and speaking with credit card companies to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Trager remains at a substantial and imminent risk of future harm.

### **SOUTH DAKOTA**

82. Plaintiff Charles Hanson is a resident of the State of South Dakota and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Hanson spent time and money purchasing identity theft protection services in order to mitigate against potential harm. In addition, as a result of the Data Breach, Plaintiff Hanson spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Hanson remains at a substantial and imminent risk of future harm.

### **TENNESSEE**

83. Plaintiff Douglas Blake is a resident of the State of Tennessee and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Blake spent time and effort monitoring his financial accounts to detect fraudulent activity and contacting credit card companies to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Blake remains at a substantial and imminent risk of future harm.

**TEXAS**

84. Plaintiff John Stephen Griesenbeck is a resident of the State of Texas and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Griesenbeck also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Griesenbeck has suffered fraud in the form of having his checking account compromised by an unauthorized individual. As a result of this fraud, Plaintiff Griesenbeck spent significant time and effort dealing with the fraud including obtaining a new checking account, credit card, notifying creditors, changing account information on numerous other accounts set up to auto-pay from his checking account, and monitoring his credit accounts on a regular basis. In addition, as a result of the Data Breach, Plaintiff Griesenbeck spent time and money reviewing his financial records and enrolling in credit monitoring and identity theft protection services to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Griesenbeck remains at a substantial and imminent risk of future harm.

85. Plaintiff Michael Piana is a resident of the State of Texas and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Piana has suffered identity theft and fraud in the form of an unauthorized account opened under his name at a credit union, and the use of that account to pay for a significant charge at a jewelry store. As a result of this identity theft and fraud, Plaintiff Piana spent time calling and emailing the credit union to mitigate against potential harm. Given the highly sensitive nature of the information stolen, Plaintiff Piana remains at a substantial and imminent risk of future harm.

86. Plaintiff Hope Turner is a resident of the State of Texas provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Turner has suffered identity theft and fraud in the form of an

unsecured loan taken out in her name. Plaintiff Turner also had several mobile accounts opened in her name. As a result of this identity theft and fraud, Plaintiff Turner spent time on the phone with banks, completing identify theft and police reports, copying personal records, changing passwords, checking credit alerts, and trying to determine the identity of individuals fraudulently using her information. In addition, as a result of the Data Breach, Plaintiff Turner spent time and money purchasing credit monitoring, freezing her accounts in order to mitigate against future potential harm, and monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Turner remains at a substantial and imminent risk of future harm.

#### **UTAH**

87. Plaintiff Gary Dean Dittmore is a resident of the State of Utah and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Dittmore also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Dittmore has suffered identity theft in the form of an unauthorized automobile loan applied for in his name. As a result of this identity theft, Plaintiff Dittmore spent time and money attempting to address the fraud and purchasing identity theft protection services in order to mitigate against further potential harm. In addition, as a result of the Data Breach, Plaintiff Dittmore spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Dittmore remains at a substantial and imminent risk of future harm.

#### **VERMONT**

88. Plaintiff Michael Charron is a resident of the State of Vermont and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Charron spent time and money addressing suspicious

activity, contacting his credit card companies and closing accounts, and taking other steps to help mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Charron remains at a substantial and imminent risk of future harm.

89. Plaintiff Jeninne Pitts is a resident of the State of Vermont and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Pitts spent time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly sensitive nature of the information stolen, Plaintiff Pitts remains at a substantial and imminent risk of future harm.

### **VIRGINIA**

90. Plaintiff Shantonu Kundu is a resident of the Commonwealth of Virginia and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Kundu spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Kundu remains at a substantial and imminent risk of future harm.

91. Plaintiff James Marshall Farmer is a resident of the Commonwealth of Virginia and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Farmer spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Farmer remains at a substantial and imminent risk of future harm.

### **WASHINGTON**

92. Plaintiff Thomas Evankovich is a resident of the State of Washington and provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. Plaintiff Evankovich also provided his passport information in order to stay at a Marriott Property. As a result of the Data Breach, Plaintiff Evankovich spent time and effort monitoring his financial

accounts to detect fraudulent activity and speaking with his bank to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Evankovich remains at a substantial and imminent risk of future harm.

#### **WEST VIRGINIA**

93. Plaintiff Harry Bell is a resident of the State of West Virginia and provided his Personal Information to Marriott in order to purchase Marriott timeshares and stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Bell has suffered identity theft in the form of an unauthorized account opened in his name. As a result of this identity theft, Plaintiff Bell spent time filing a police report and contacting the company to close the fraudulent account. In addition, as a result of the Data Breach, Plaintiff Bell spent time and effort monitoring his financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Bell remains at a substantial and imminent risk of future harm.

#### **WISCONSIN**

94. Plaintiff Gertie Haese is a resident of the State of Wisconsin and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Haese spent time and effort monitoring her financial accounts to detect fraudulent activity and speaking with her credit card company to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Haese remains at a substantial and imminent risk of future harm.

#### **WYOMING**

95. Plaintiff Amber Flor is a resident of the State of Wyoming and provided her Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach. As a result of the Data Breach, Plaintiff Flor spent time and effort monitoring her accounts for

fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Flor remains at a substantial and imminent risk of future harm.

### **FACTUAL ALLEGATIONS**

#### ***Marriott International and its Privacy Policy***

96. Marriott International is a multinational, diversified hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities, including 30 brands with more than 7,000 properties across 130 countries and territories globally. Founded in 1927, the company is headquartered in Bethesda, Maryland, and maintains hotel brands including Marriott, Courtyard, and Ritz-Carlton. Marriott reported revenues of \$20.75 billion in the 2018 fiscal year.

97. Marriott International was founded by J. Willard Marriott and is now led by his son, Executive Chairman Bill Marriott, and President and CEO Arne Sorenson.

98. On September 23, 2016, Marriott International closed a \$13.6 billion acquisition of Starwood Hotels & Resorts Worldwide, bringing together its Marriott, Courtyard, and Ritz-Carlton brands with Starwood's Sheraton, Westin, W Hotels, and St. Regis properties. As a result, the 30 hotel brands that now fall under Marriott International's umbrella have made it the largest hotel chain in the world, accounting for 1 out of every 15 hotel rooms globally.

99. Guests can make reservations at a Marriott hotel via multiple methods, including through Marriott's website. When making a reservation, Marriott requires the guest to provide certain personal information including name, address, email address, phone number, and payment card information. In some instances, Marriott also collects passport information, room preferences, travel destinations, and other personal information.

100. In Marriott's Global Privacy Statement dated May 18, 2018, Marriott represents that: "The Marriott Group, which includes Marriott International, Inc., Starwood Hotels & Resorts

Worldwide, LLC ... and their affiliates, values you as our guest and recognizes that privacy is important to you.” It explains that the Marriott Group collects data:

- through websites operated by us from which you are accessing this Privacy Statement, including Marriott.com and other websites owned or controlled by the Marriott Group (collectively, the “**Websites**”)
- through the software applications made available by us for use on or through computers and mobile devices (the “**Apps**”)
- through our social media pages that we control from which you are accessing this Privacy Statement (collectively, our “**Social Media Pages**”)
- through HTML-formatted email messages that we send you that link to this Privacy Statement and through your communications with us
- when you visit or stay as a guest at one of our properties, or through other offline interactions.

101. The Privacy Statement defines “Collection of Personal Data” as follows:

“**Personal Data**” are data that identify you as an individual or relate to an identifiable individual. At touchpoints throughout your guest journey, we collect Personal Data in accordance with law, such as:

- Name
- Gender
- Postal address
- Telephone number
- Email address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference
- Date and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data

- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

102. Marriott states that “in more limited circumstances, we also may collect” the following:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel
- Guest preferences, inquiries and comments and any other personalized data (“**Personal Preferences**”), such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit.

103. Marriott further represents that: “We seek to use reasonable organizational, technical and administrative measures to protect Personal Data.”

104. Marriott recognizes the value of this information as evidenced by the fact that Marriott employs a customer analytics company for the systematic examination of its customer information to identify, attract, and retain the most profitable customers and to predict future behaviors. According to Marriott, “there is no lack of available data: household profile, including number of kids; type of jobs held by family members; their salaries; where and how they spend their money and even the type of jeans they buy.”<sup>1</sup>

---

<sup>1</sup> D. Eisen, *Marriott Bets on Predictive Analytics for Brand Growth*, QUESTEX LLC (Jan. 31, 2018), <https://www.hotelmanagement.net/tech/marriott-builds-its-brands-by-knowing-more-about-you> (last accessed July 22, 2019).

105. Knowing the significant value and sensitive nature of the information it collects, Marriott's current privacy policy represents that Marriott uses "reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information."<sup>2</sup>

### ***Starwood Hotels and Its Preferred Guest Program***

106. Starwood Hotels was originally formed by Starwood Capital Partners, a Chicago-based real estate investment firm founded by Barry Sternlicht in 1991.

107. In 1995, Starwood Capital acquired Hotel Investors Trust and Hotel Investors Corporation, one of a handful of public companies that was grandfathered in as a "paired-share" real estate investment trust ("REIT"). This structure allowed Starwood to own and operate its hotels through a single entity, while at the same time taking advantage of favorable tax shelter aspects of a REIT.

108. This preferred tax status garnered significant investment in Starwood Capital and by 1998, it was able to acquire established hotel brands like Westin for \$1.57 billion and ITT Sheraton Corporation for \$9.8 billion.

109. Over the next two decades, Starwood continued its global expansion by acquiring numerous hotel chains including Le Méridien, a chain of more than 120 properties primarily located in Europe and the Middle East, and launching a number of specialty brands. Starwood brands now include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels &

---

<sup>2</sup> *Marriott U.S. Privacy Shield Guest Privacy Policy* (updated May 24, 2019), <https://www.marriott.com/about/global-privacy.mi> (last accessed July 22, 2019).

Resorts, Four Points by Sheraton, and Design Hotels. Starwood also operates certain Starwood-branded timeshare properties.

110. In 1999, Starwood launched a guest loyalty programs known as Starwood Preferred Guest Program (“SPG Program”) to create brand loyalty and encourage travelers to stay at its properties by offering rewards. Starwood promoted the SPG Program as first in the industry to offer no blackout dates, no capacity controls, and online redemption.<sup>3</sup>

111. Starwood has long touted its SPG Program as industry-leading and a significant driver of repeat business from frequent travelers. For example, in 2012, Starwood stated that the SPG Program, “...launches the richest elite program benefits in history for global mega travelers including standouts like first-of-its-kind 24-hour check-in, confirmable upgrades, and free breakfast. For our most loyal guests, SPG offers lifetime status and a dedicated Starwood ambassador. In its first year, SPG transformation drove a 12% year-over-year increase in revenue to our hotels from SPG members with a 16% increase from Platinum members.”<sup>4</sup>

112. Starwood also promoted the SPG Program’s “crossover rewards” with companies such as Delta Airlines and convenience features such as keyless entry that “enable guests to bypass the front desk, avoid waiting in line and ultimately unlock their stay with a simple tap of their smartphone.”<sup>5</sup>

113. In the course of its business, Starwood collects and stores significant amounts of sensitive customer information. For example, Starwood’s online privacy statement dated October 15, 2014 stated that Starwood is “dedicated to protecting your privacy and safeguarding your

---

<sup>3</sup> *Starwood Corporate Overview*, at 9-10, <https://marriott.gcs-web.com/static-files/4cb4e011-ddff-4613-984f-1e08d799227c> (last accessed July 22, 2019).

<sup>4</sup> *Id.*, at 5.

<sup>5</sup> *Id.*, at 4.

personally identifiable information” and “collects information about our guests and visitors to our web sites so that we can provide an experience that is responsive to our guests’ and visitors’ needs.”

The statement further provided:

**TYPES OF INFORMATION WE COLLECT:**

Starwood collects information about our guests and visitors to our web sites so that we can provide an experience that is responsive to our guests’ and visitors’ needs. Information may be collected as part of: (i) fulfilling reservation or information requests, (ii) purchasing products or services, (iii) registering for program membership, (iv) submitting a job application, (v) responding to communications from us (e.g., surveys, promotional offers, or reservation confirmations), (vi) accommodating your personal preferences, (vii) fulfilling requests for services or recommendations we provide you, (viii) working with third party sources, including collecting information available from social networking and other web sites, to better assist us with understanding your interests and to serve you better, (ix) your use of our apps on your electronic devices, (x) updating your contact information including your address (through such services as the National Change of Address Service in the United States), or (xi) facilitating the transmission of forward to a friend email at your request. The types of personally identifiable information (sometimes referred to as “PII”) that we collect may include your name, home, work and e-mail addresses, telephone, mobile telephone, and fax numbers, credit card information, date of birth, gender, and lifestyle information such as room preferences, leisure activities, names and ages of children, and other information necessary to fulfill special requests (e.g., health conditions that require special room accommodations).

Starwood may also collect non-personally identifiable information about you, such as your use of our web sites, communication preferences, travel habits, aggregated data relative to your stays, and responses to promotional offers and surveys.

\*\*\*

**PURPOSE FOR COLLECTION, PROCESSING, AND DISCLOSURE:**

**Collection & Use**

Starwood is fully committed to providing you with information about the collection and use of PII furnished by, or collected from, visitors while using our web sites, products and services. It is our practice not to ask you for information unless we need it or intend to use it. Some of the primary purposes for collecting your PII are as follows:

- providing services such as processing a transaction (e.g., making a reservation, fulfilling a request for information, or completing a product order)

- marketing and communications with you in relation to the products and services offered by Starwood, our strategic marketing partners, and other trusted third parties
- performing market research via surveys to better serve your needs, improve the effectiveness of our web sites, your hotel experience, our various types of communications, advertising campaigns, and/or promotional activities

\*\*\*

### **Processing and Disclosure**

In most cases, the information you provide is added to a local or global database. In the course of processing your information, it may be necessary to transfer your PII to Starwood's affiliates, properties within the Starwood system and/or third party service providers located in the United States and throughout the world for the purposes outlined within this Privacy Statement. Unless otherwise precluded or governed by legal requirements and/or process, Starwood subsidiaries, affiliates and property owners that may receive your information are required to abide by substantially similar privacy requirements relating to your PII. As a general practice, Starwood does not sell, rent, or give physical possession of your PII to unaffiliated third parties outside the Starwood system. Situations in which Starwood may disclose your information to others include:

- when we have received your consent to do so
- in situations where sharing or disclosing your information is required in order to offer you products or services you desire (e.g., a vacation package)
- when companies or services providers that perform business activities on behalf of Starwood require such information (e.g., credit card processing, customer support services, market research administration or database management services)
- when a hotel or other property leaves the Starwood system and access to your PII is necessary to facilitate business operations or meet contractual obligations in connection with the fulfillment of reservations that are booked for future stays or events
- in the event Starwood is merged or acquired by another company
- to comply with legal or regulatory requirements or obligations in accordance with applicable law, a court order or a subpoena
- in case of emergency such as to safeguard the life, health, or property of an individual

If information is shared as mentioned above, we seek to limit the scope of information that is furnished to the amount necessary for the performance of the specific function. Unless otherwise precluded by legal process, we require third parties to protect your PII and abide by applicable privacy laws and regulations.

\*\*\*

#### DATA TRANSFERS ACROSS INTERNATIONAL BORDERS:

As a global company, we endeavor to provide you with the same outstanding service in New York City, as you would find in Paris or Beijing. To achieve this goal, we have established a global network comprised of properties, offices, data centers, trusted marketing partners, service providers, customer contact centers, and trained associates around the globe. The nature of our business and our operations require us to transfer your information, including PII, to other group companies, properties, centers of operations, data centers, or service providers that may be located in countries outside of your own. We may transfer the PII we collect about you to countries other than the country in which the information was originally collected. Although the data protection and other laws of these various countries may not be as comprehensive as those in your own country, Starwood will take appropriate steps to ensure that your PII is protected and handled as described in this Privacy Statement.

\*\*\*

#### SECURITY SAFEGUARDS:

Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your PII against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although “guaranteed security” does not exist either on or off the Internet, we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, “firewalls” and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit.

114. Although Starwood represented that it “recognized the importance of keeping its valuable customer information secure” and had “security measures in place to help protect” consumers against “unauthorized access” of their Personal Information—it failed to live up to that promise by failing to implement and maintain reasonable safeguards that resulted in the exposure and exfiltration of the Personal Information for hundreds of millions of hotel guests.

#### *Marriott’s Acquisition of Starwood*

115. On November 16, 2015, Marriott International announced that it was purchasing Starwood for \$13.6 billion, creating the world’s largest hotel company.

116. After the transaction closed on September 23, 2016, Marriott stated in a press release that the new company “offers the most comprehensive portfolio of brands including leading lifestyle brands, a significant global footprint, and leadership in the luxury and select-service tiers as well as the convention and resort segment. Beginning today, Marriott will match member status across Marriott Rewards – which includes The Ritz-Carlton Rewards – and Starwood Preferred Guest (SPG), enabling members to transfer points between the programs for travel and exclusive experiences when they link their accounts later today.”<sup>6</sup>

117. The press release further stated that Marriott “will operate or franchise more than 5,700 properties and 1.1 million rooms, representing 30 leading brands from the moderate-tier to luxury in over 110 countries. With the completion of this acquisition, Marriott’s distribution has more than doubled in Asia and the Middle East & Africa combined.”<sup>7</sup>

118. According to Marriott CEO Arne Sorenson, Starwood’s SPG Program was a “central, strategic rationale for the transaction” because its members are deeply loyal, have generally higher incomes, and tend to spend many nights on the road.<sup>8</sup>

119. In any acquisition of this size, it is standard practice to perform cybersecurity due diligence, including researching undisclosed or unknown data breaches, as well as identifying information technology (“IT”) security risks and shortfalls in operations and governance of the target company. A primary responsibility of Marriott (or any company conducting a merger and

---

<sup>6</sup> <https://news.marriott.com/2016/09/marriotts-acquisition-of-starwood-complete/> (last accessed July 22, 2019).

<sup>7</sup> *Id.*

<sup>8</sup> S. Mayerowitz, *Marriott Buys Starwood, Becoming World’s Largest Hotel Chain*, THE ASSOCIATED PRESS (Sept. 23, 2016), <https://apnews.com/a082e1af32ee4fd6a35e0542461c5b79> (last accessed July 22, 2019).

acquisition) is to perform a full and complete cyber-security assessment to understand the state of the target company's computer networks, systems, and its vulnerabilities.

120. During the year that elapsed between announcement and closing of the merger, Marriott and Starwood retained respective financial advisors and legal counsel to analyze business records and make a financial assessment of the merger and valuation of the stock for purposes of recommending the merger to stockholders. [REDACTED]

[REDACTED] even after Starwood disclosed a breach of its point of sale systems at more than 50 locations just four days after Marriott's announcement of the merger.

121. This lack of cybersecurity due diligence [REDACTED]

122. After the Data Breach, Jeff Flaherty, a senior director of global communications and public affairs at Marriott, stated that "as part of the company's integration efforts, Marriott conducted an assessment of the legacy Starwood IT systems prior to and after the close of the transaction."<sup>9</sup>

---

<sup>9</sup> *Starwood Data Breach: Lessons for the Hotel Industry*, HOTEL NEWS NOW (Apr. 9, 2019), <http://www.hotelnewsnow.com/Articles/294646/Starwood-data-breach-Lessons-for-the-hotel-industry> (last accessed July 22, 2019).

123. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>10</sup>

124. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>11</sup> [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>12</sup> [REDACTED]

125. [REDACTED]

[REDACTED]

[REDACTED]<sup>13</sup>

---

<sup>10</sup> [REDACTED]

<sup>11</sup> [REDACTED]

<sup>12</sup> [REDACTED]

<sup>13</sup> [REDACTED]

126. [REDACTED]

[REDACTED]

[REDACTED]<sup>14</sup>

127. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>15</sup>

128. [REDACTED]

[REDACTED]

[REDACTED]

129. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>16</sup>

130. In March 2017, Marriott internally announced “Project Tetris” – which referred to Marriott’s planned integration of Starwood properties into Marriott’s finance model. It was one of

---

<sup>14</sup> [REDACTED]

<sup>15</sup> [REDACTED].

<sup>16</sup> [REDACTED]

many expected initiatives directed specifically at Starwood-branded hotel owners.<sup>17</sup> Project Tetris outlined the transition plan and savings anticipated as a result of leveraging Marriott's size and scale to improve negotiated merchant contracts and achieve incremental savings through increased buying power.<sup>18</sup>

131. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>19</sup>

132. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>20</sup>

---

<sup>17</sup> A. Leber, *How Marriott Plans to Save Starwood Owners Real Money*, QUESTEX, LLC (Mar. 28, 2017), <https://www.hotelmanagement.net/asset-management/how-marriott-plans-to-save-starwood-owners-real-money> (last accessed July 22, 2019).

<sup>18</sup> *Id.*

<sup>19</sup> [REDACTED]

<sup>20</sup> [REDACTED]

133. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>21</sup> [REDACTED]

[REDACTED]

134. Marriott ultimately launched its new loyalty program on August 18, 2018, combining Starwood's SPG Program with Marriott Rewards and Ritz-Carlton Rewards onto the Marriott IT platform.<sup>22</sup> The platform migration did not go smoothly. During this time, the systems were down sporadically, the nomenclature and status were confusing to members from different programs, and many Marriott members ended up with an incorrect status.<sup>23</sup>

135. In fact, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>24</sup>

136. Marriott's cybersecurity due diligence fell woefully short as Marriott [REDACTED] failed to detect numerous red flags indicating that Starwood's network had already been breached.

---

<sup>21</sup> [REDACTED]

<sup>22</sup> G. Leff, *Marriott Explains What Systems Still Aren't Working and When They'll Be Fixed*, VIEW FROM THE WING (Aug. 27, 2018), <https://viewfromthewing.boardingarea.com/2018/08/27/marriott-explains-what-systems-still-arent-working-and-when-theyll-be-fixed/> (last accessed July 22, 2019).

<sup>23</sup> *Id.*

<sup>24</sup> [REDACTED]

137. For example, Marriott and Starwood [REDACTED]

[REDACTED]<sup>25</sup>

[REDACTED]<sup>26</sup>

[REDACTED]<sup>27</sup>

138. [REDACTED]

Marriott could have thwarted the Data Breach or at the very least discovered the hackers lurking in the Starwood's networks long before they were able to remove the Starwood guest reservation database tables containing the Personal Information of 383 million guests.

***Marriott and Starwood Knew they were Targets of Cyber Threats***

139. Both before and after the acquisition, Marriott knew it and other hotel chains were prime targets for hackers given the significant amount of sensitive customer information it collects in the course of business. In fact, both Starwood and Marriott, among many other high-profile hotel chains, were *targeted* in other data breaches by hackers in the months and years before the Data Breach was discovered.

140. On February 3, 2014, White Lodging Services Corporation, a franchise management company used by Marriott and Starwood, announced that the POS systems at 14 hotels, including seven Marriott locations, one Westin location, and one Sheraton location, were

---

<sup>25</sup> [REDACTED]

<sup>26</sup> [REDACTED]

<sup>27</sup> [REDACTED]

compromised. White Lodging’s statement confirmed that the “unlawfully accessed data may have included names printed on customers’ credit or debit cards, credit or debit card numbers, the security code and card expiration dates.”<sup>28</sup>

141. Following confirmation of that breach, Marriott also issued a statement stating that “one of its franchisees has experienced unusual fraud patterns in connection with its systems that process credit card transactions at a number of hotels across a range of brands, including some Marriott-branded hotels.” The statement continued: “As this impacts customers of Marriott hotels we want to provide assurance that Marriott has *a long-standing commitment to protect the privacy of the personal information that our guests entrust to us*, and we will continue to monitor the situation closely.”<sup>29</sup>

142. The following year, sources in the banking industry began seeing a pattern of fraud on payment cards that were used at Marriott hotels. On April 8, 2015, White Lodging again confirmed that its POS systems at 10 hotels were breached, this time including seven Marriott locations and one Sheraton location.

143. Following this second breach, White Lodging issued another statement: “After suffering a malware incident in 2014, we took various actions to prevent a recurrence, including engaging a third party security firm to provide security technology and managed services,” said Dave Sibley, White Lodging president and CEO, Hospitality Management. “These security measures were unable to stop the current malware occurrence on point of sale systems at food and

---

<sup>28</sup> N. Vivion, *White Lodging Releases More About Credit Card Data Breach, Including Affected Hotels*, PHOCUSWIRE (Feb. 4, 2014), <https://www.phocuswire.com/White-Lodging-releases-more-about-credit-card-data-breach-including-affected-hotels> (last accessed July 22, 2019).

<sup>29</sup> B. Krebs, *Hotel Franchise Firm White Lodging Investigates Breach*, KREBS ON SECURITY (Jan. 31, 2014), <https://krebsonsecurity.com/2014/01/hotel-franchise-firm-white-lodging-investigates-breach/> (emphasis added) (last accessed July 22, 2019).

beverage outlets in 10 hotels that we manage. We continue to remain committed to investing in the measures necessary to protect the personal information entrusted to us by our valuable guests. We deeply regret and apologize for this situation.”

144. Marriott spokesperson Jeff Flaherty also commented on the White Lodging breach: “We recently were made aware of the possibility of unusual credit card transactions at a number of hotels operated by one of our franchise management companies. We understand the franchise company is looking into the matter. Because the suspected issue is related to systems that Marriott does not own or control, we do not have additional information to provide.”<sup>30</sup>

145. On November 20, 2015, just four days after the announcement of Marriott’s acquisition of Starwood, Starwood disclosed that its point-of-sale (“POS”) systems at 54 hotels located across North America were infected with malware (malicious software designed to cause damage to a computer, server, client, or computer network), enabling unauthorized parties to access the payment card data of its customers.<sup>31</sup>

146. In a letter to Starwood customers, Starwood stated that the “malware was designed to collect certain payment card information, including cardholder name, payment card number, security code and expiration date” and Starwood “engaged third-party forensic experts to conduct an extensive investigation” but there was “no indication that our guest reservation or Starwood Preferred Guest membership systems were impacted.” It is unclear what type of “extensive investigation” occurred as Marriott’s latter statement proved to be false given that hackers had access to Starwood’s guest reservation database as early as July 2014.

---

<sup>30</sup> B. Krebs, *Banks: Card Thieves Hit White Lodging Again*, KREBS ON SECURITY (Feb. 3, 2015), <https://krebsonsecurity.com/2015/02/banks-card-thieves-hit-white-lodging-again/#more-29697> (last accessed July 22, 2019).

<sup>31</sup> [https://oag.ca.gov/system/files/starwood-notice-materials\\_0.pdf](https://oag.ca.gov/system/files/starwood-notice-materials_0.pdf) (last accessed July 22, 2019).

147. In another example, a security researcher found an SQL injection bug (type of attack that can give malicious actor control over target's database by inserting arbitrary code into a database query) that could have been exploited to gain access to Starwood databases. The researcher said that such vulnerabilities and services offering to hack Starwood were being offered for sale on underground websites in 2014.<sup>32</sup>

148. In June 2017, Marriott's security team was notified by independent cybersecurity researchers that hackers were able to access the email servers of Marriott's Computer Incident Response Team ("CIRT") due to an external analyst downloading a malware sample.<sup>33</sup>

149. A Marriott spokesperson told *Forbes* the breach "was an isolated incident involving that one analyst's machine that had access to Marriott's outlook Web access mailbox but was not connected to the Marriott network."<sup>34</sup> Daniel Gallagher, an independent cybersecurity researcher, uncovered the 2017 breach when he located the server on which Nigerian hackers were running their criminal enterprise.<sup>35</sup>

150. SecureWorks, a cybersecurity provider, was the vendor during the 2017 breach in which Marriott's CIRT was compromised.<sup>36</sup> At the time, SecureWorks declined to comment and Marriott declined to name the contractor.<sup>37</sup>

---

<sup>32</sup> T. Brewster, *Revealed: Marriott's 500 Million Hack Came After a String of Security Breaches*, FORBES (Dec. 3, 2018), <https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#27ac9dd546f4> (last accessed July 22, 2019).

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

151. In yet another example, security researcher Alex Holden discovered that six servers hosting starwoodhotels.com domains were controlled by a Russian botnet (a network of private computers infected with malicious software and controlled as a group without the owner's knowledge). Holden also detailed other security concerns, including that one of Starwood's cloud portals had an easily guessable password, which could allow hackers to access financial records, IT security controls, and booking information.<sup>38</sup>

152. It is not surprising that hotels have been frequent targets for hackers. As noted by one cybersecurity expert, "hotels are an attractive target for hackers because they hold a lot of sensitive information, including credit card and passport details, but often don't have security standards as tough as those of more regulated industries, like banking."<sup>39</sup>

153. In its recent Data Breach Investigations Report, Verizon noted that 15% of all data breaches occurring in 2017 involved the accommodation and food services industry and that it is "the hardest hit" industry for POS intrusions.<sup>40</sup> The report noted that there were 338 breaches in the accommodation industry in 2017 alone, including at major hotel brands including Hyatt, Radisson, Hard Rock, and Kimpton, among others.<sup>41</sup>

154. For example, on October 30, 2018, Radisson Hotels disclosed a data breach affecting Radisson Rewards members who had their names, company names, e-mail addresses,

---

<sup>38</sup> *Id.*

<sup>39</sup> Democrat-Gazette Staff Wire Reports, *Breach Puts Hotel Guests' Data at Risk*, ARKANSAS DEMOCRAT GAZETTE (Dec. 1, 2018), <https://www.arkansasonline.com/news/2018/dec/01/breach-puts-hotel-guests-data-at-risk-2/> (last accessed July 22, 2019).

<sup>40</sup> Verizon 2018 Data Breach Investigations Report, 11th Ed., at 5, 24, 25, 27, 28, [https://enterprise.verizon.com/resources/reports/DBIR\\_2018\\_Report.pdf](https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf) (last accessed July 22, 2019).

<sup>41</sup> *Id.*

addresses, phone numbers, Radisson Rewards member numbers, and frequent flyer numbers accessed by an unauthorized party.<sup>42</sup>

155. In August 2018, it was announced that China-based Huazhu Hotels Group suffered a massive data breach where the personal information of hundreds of millions of hotel guests was exfiltrated and offered for sale on the dark web.<sup>43</sup>

156. In November 2017, Hilton Worldwide Holdings Inc. agreed to pay \$700,000 and bolster its data security practices for mishandling data breaches in 2014 and 2015, including failing to maintain reasonable data security and failing to notify victims of the data breach in a timely manner. The breaches, discovered in February and July 2015, respectively, exposed the credit card numbers of more than 360,000 guests.<sup>44</sup>

157. In October 2017, Hyatt announced that it discovered unauthorized access to payment card information at 41 of its properties worldwide. This announcement came on the heels of Hyatt's announcement in late 2015 that hackers had gained access to credit card systems at 250 properties in 50 different countries for a period spanning nearly four months, exposing customers' payment card data including cardholder names, numbers, expiration dates, and internal verification codes.<sup>45</sup>

---

<sup>42</sup> C. Osborne, *Radisson Hotel Group Suffers Data Breach, Customer Info Leaked*, ZDNET (Nov. 1, 2018), <https://www.zdnet.com/article/radisson-hotel-group-chain-suffers-data-breach/> (last accessed July 22, 2019).

<sup>43</sup> E. Hertzfeld, *Data Leak from Huazhu Hotels May Affect 130 Million Customers*, QUESTEX, LLC (Aug. 30, 2018), <https://www.hotelmanagement.net/tech/data-leak-from-huazhu-hotels-may-affect-130-million-customers> (last accessed July 22, 2019).

<sup>44</sup> J. Stempel, *Hilton to Pay \$700,000 Over Credit Card Data Breaches*, REUTERS (Oct. 31, 2017), <https://www.reuters.com/article/us-hilton-wrldwide-settlement/hilton-to-pay-700000-over-credit-card-data-breaches-idUSKBN1D02L3> (last accessed July 22, 2019).

<sup>45</sup> B. Krebs, *Hyatt Hotels Suffers 2nd Card Breach in 2 Years*, KREBS ON SECURITY (Oct. 17, 2017), <https://krebsonsecurity.com/2017/10/hyatt-hotels-suffers-2nd-card-breach-in-2-years/> (last accessed July 22, 2019).

158. In July 2017, multiple hotel chains including Hard Rock Hotels & Casinos, Four Seasons Hotels and Resorts, Trump Hotels, Loews Hotels, Kimpton Hotels & Restaurants, RLH Corporation, and Club Quarter Hotels, among others, reported a data breach via a third-party reservations system provided by Sabre Hospitality Solutions. The breach permitted unauthorized access to customers' credit card information and certain reservation information between August 2016 and March 2017.<sup>46</sup>

159. In February 2017, InterContinental Hotels Group announced that cash registers at more than 1,000 of its properties were infected with malware designed to siphon customers' payment card data from on-site hotel locations between September 29, 2016 and December 29, 2016.<sup>47</sup>

160. In September 2016, Kimpton Hotel & Restaurant Group LLC announced that customers' payment card information was compromised by malware installed on its servers at more than 60 of its hotels and restaurants during a six-month period.<sup>48</sup>

161. In June 2016, Hard Rock Hotel & Casino Las Vegas announced that after receiving reports of fraudulent activity associated with payment cards used at its hotel, the resort conducted

---

<sup>46</sup> D. Ting, *Data Breach at Sabre Hits Four Seasons and Other Hotels*, SKIFT (July 11, 2017), <https://skift.com/2017/07/11/data-breach-at-sabre-hits-four-seasons-and-other-hotels/> (last accessed July 22, 2019); B. Krebs, *Breach at Sabre Corp.'s Hospitality Unit*, KREBS ON SECURITY (May 17, 2017) <https://krebsonsecurity.com/2017/05/breach-at-sabre-corp-s-hospitality-unit/> (last accessed July 22, 2019).

<sup>47</sup> M. Schwartz, *InterContinental Hotels Group: Malware Hit 1,200 Locations*, BANK INFO SECURITY (Apr. 19, 2017), <https://www.bankinfosecurity.com/intercontinental-hotels-group-malware-hit-1200-locations-a-9852> (last accessed July 22, 2019).

<sup>48</sup> B. Krebs, *Kimpton Hotels Acknowledges Data Breach*, KREBS ON SECURITY (Sept. 16, 2017), <https://krebsonsecurity.com/2016/09/kimpton-hotels-acknowledges-data-breach/> (last accessed July 22, 2019).

an investigation revealing that malware had been installed on its servers allowing unauthorized access to customers' names, credit card numbers, expiration dates, and verification numbers.<sup>49</sup>

162. The following month, Omni Hotels & Resorts confirmed that a similar malware attack exposed the names and payment card information of more than 50,000 customers at 49 of its properties.<sup>50</sup>

163. In November 2015, Noble House Hotels and Resorts announced a breach affecting six of its properties over different periods of time from December 29, 2014 to August 11, 2015. This breach also involved malware installed on Noble's POS systems.<sup>51</sup>

164. In March 2015, hotel chain Mandarin Oriental Hotel Group confirmed that its hotels were affected by a payment card breach indicating that some of the chain's POS systems were infected with malware capable of stealing customer card data.<sup>52</sup>

165. Despite these well-publicized breaches of their competitors, Marriott and Starwood failed to undertake adequate analyses and testing of their own systems to ensure that similar vulnerabilities were remedied.

---

<sup>49</sup> S. Ragan, *Hard Rock Las Vegas Suffers a Second Data Breach*, CSO ONLINE (June 28, 2016), <https://www.csoonline.com/article/3089449/hard-rock-las-vegas-suffers-a-second-data-breach.html> (last accessed July 22, 2019).

<sup>50</sup> K. Robinson, *Dallas-based Omni Hotels Announces Data Breach of 50,000 Credit, Debit Cards*, THE DALLAS MORNING NEWS (July 2016), <https://www.dallasnews.com/business/hotels/2016/07/12/omni-hit-data-breach-impacted-50000-credit-debit-cards> (last accessed July 22, 2019).

<sup>51</sup> HNN Editorial Staff, *Timeline: The Growing Number of Hotel Data Breaches*, HOTEL NEWS NOW (Nov. 30, 2018) <http://www.hotelnewsnow.com/Articles/50937/Timeline-The-growing-number-of-hotel-data-breaches> (last accessed July 22, 2019).

<sup>52</sup> B. Krebs, *Credit Card Breach at Mandarin Oriental*, KREBS ON SECURITY (March 4, 2015), <https://krebsonsecurity.com/2015/03/credit-card-breach-at-mandarian-oriental/> (last accessed July 22, 2019).

166. In addition to data breaches affecting the hospitality industry, Marriott and Starwood observed numerous, well-publicized data breaches involving other types of major corporations who were also targeted given the sensitive consumer information they retained.

167. For example, through a series of data breaches extending back to 2013, more than three billion Yahoo! user accounts were compromised when account-holders' names, addresses, and dates of birth were stolen. The hackers also stole users' passwords, both encrypted and unencrypted, and security questions and answers.<sup>53</sup>

168. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target and the Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.<sup>54</sup>

169. In early 2015, Anthem, Inc., the second-largest health insurer in the United States, suffered a data breach that exposed the names, addresses, Social Security numbers, dates of birth, and employment histories of nearly 80 million current and former plan members.<sup>55</sup> Other health care providers like, Premera and Excellus BlueCross BlueShield, reported similar breaches.<sup>56</sup>

---

<sup>53</sup> S. Larson, *Every Single Yahoo Account was Hacked – 3 Billion in All*, CNN (Oct. 4, 2017), <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html> (last accessed July 22, 2019).

<sup>54</sup> B. Krebs, *Home Depot Hit By Same Malware as Target*, KREBS ON SECURITY (Sept. 14, 2014), <https://krebsonsecurity.com/tag/home-depot-databreach/> (last accessed July 22, 2019).

<sup>55</sup> C. Riley, *Insurance Giant Anthem Hit by Massive Data Breach*, CNN (Feb. 6, 2015), <https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/> (last accessed July 22, 2019).

<sup>56</sup> *Cyber Breach Hits 10 Million Excellus Healthcare Customers*, USA TODAY (Sept. 10, 2015), <https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/> (last accessed July 22, 2019).

170. In September 2017, credit reporting agency Equifax announced that hackers stole the personal and financial information of nearly 150 million Americans between May and July 2017.<sup>57</sup>

171. Despite being holders of Personal Information for millions of individuals worldwide, Defendants failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly-sensitive databases. Defendants had the resources to prevent a breach and made significant expenditures to market their hotels and hospitality services, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting the hospitality and similar industries.

#### *The Data Breach*

172. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>58</sup> [REDACTED]

[REDACTED]

[REDACTED]

173. [REDACTED]

[REDACTED]

[REDACTED]<sup>59</sup> [REDACTED]

---

<sup>57</sup> <https://www.equifaxsecurity2017.com/frequently-asked-questions/> (last accessed July 22, 2019).

<sup>58</sup> [REDACTED]

<sup>59</sup> [REDACTED]

[REDACTED]

[REDACTED]

174. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>60</sup>

175. [REDACTED]

[REDACTED]

[REDACTED]<sup>61</sup> [REDACTED]

[REDACTED]

[REDACTED]<sup>62</sup> [REDACTED]

[REDACTED]<sup>63</sup>

176. [REDACTED]

[REDACTED]

---

<sup>60</sup> [REDACTED]

<sup>61</sup> [REDACTED]

<sup>62</sup> [REDACTED]

<sup>63</sup> [REDACTED]

[REDACTED]

[REDACTED]

177. [REDACTED]

[REDACTED] This activity resulted in Accenture—the IT company tasked with managing the Starwood guest reservation database—receiving an alert that was generated by one of its security products, IBM “Guardium.” Guardium is used to provide “automated, sensitive data discovery and classification, real-time data activity monitoring and cognitive analytics to discover unusual activity around sensitive data.”<sup>65</sup>

178. On September 8, 2018, Accenture notified Marriott’s IT team that Guardium detected an anomaly in the Starwood database: an unusual query from an administrator’s account to return the count of rows from a table in the database.<sup>66</sup> The query was suspicious because the software that runs over the database does not usually need to make queries, and therefore indicated a human operator was likely manually making this (very specific) query.<sup>67</sup>

179. [REDACTED]

[REDACTED]

<sup>64</sup> [REDACTED]

<sup>65</sup> According to IBM’s Security Data Sheet, the Guardium “solution continuously monitors all data access operation in real time to detect unauthorized actions, based on detailed contextual information – the ‘who, what, where, when and how’ of each data access. Guardium Data Protection reacts immediately to help prevent unauthorized or suspicious activities by privileged insiders and potential hackers.” IBM Guardium Data Protection – *Monitor Data Access and Take Action Against Threats*, <https://www.ibm.com/us-en/marketplace/ibm-guardium-data-protection> (last accessed July 22, 2019).

<sup>66</sup> A. Sorenson, *Testimony of Arne Sorenson, President & CEO, Marriott International Before the Senate Committee on Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations*, Opening Statement (hereinafter “Sorenson Testimony”) (March 7, 2019), <https://www.hsgac.senate.gov/imo/media/doc/Soresnson%20Testimony.pdf> (last accessed July 22, 2019).

<sup>67</sup> *Id.*

[REDACTED]

180. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>68</sup>

181. After determining the individual whose credentials were used to make this query had not actually accessed the data, on September 10, 2018, Marriott “brought in third-party investigators” to look into whether the Starwood systems had been breached.<sup>69</sup> [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

182. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>68</sup> [REDACTED]

<sup>69</sup> [REDACTED]

183. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

184. The investigation revealed that the malware installed on Starwood's systems dated back to July 2014, long before the Marriott acquisition. And in early to mid-October 2018, the investigation identified additional malware, including a tool called "Mimikatz," which searches a device memory for usernames and passwords.<sup>71</sup> Yet, according to Marriott, the investigators still lacked sufficient evidence at this time that hackers had accessed customer data.<sup>72</sup>

185. Over six weeks after discovering suspicious activity on its systems, only on October 29, 2018, did Marriott finally contact the Federal Bureau of Investigation ("FBI") to notify the agency about its investigation into the unauthorized access of the Starwood servers. Just over a week later, Marriott provided the FBI with additional information including a list of the malware and IP addresses used by one or more of the hackers.

186. Marriott filed its quarterly report with the U.S. Securities and Exchange Commission ("SEC") on November 6, 2018 for the period ending September 30, 2018. The company's filing occurred after it was alerted of a potential breach on September 8, 2018, and had begun its investigation, but the filing did not contain any mention of the breach, only a description of generic cyber risk factors that had been included in previous reports.

---

<sup>70</sup> [REDACTED]

<sup>71</sup> [REDACTED]

<sup>72</sup> *Id.*

187. Marriott claims the evidence confirming the occurrence of a breach was not actually discovered until November 13, 2018, when investigators found that two compressed, encrypted files had been deleted from a device they were examining, and that those two files had potentially been removed from the Starwood network.<sup>73</sup> Marriott claims it took another six days for the investigators to decrypt the files, and on November 19, 2018, they uncovered the contents: a table of data from the Starwood guest reservation database which contained personal information of hundreds of millions of guests who had made a reservation at a Starwood property and another table containing detailed passport information.<sup>74</sup> Only then, two months later, did Marriott begin preparing to notify guests and other regulatory authorities.<sup>75</sup>

188. On November 29, 2018, Marriott provided updated information to the FBI after confirming that the attacker had accessed and exfiltrated customer data, and further notified all U.S. Attorneys General, the Federal Trade Commission (“FTC”), the SEC, regulators in 20 different countries, four major payment card networks and their credit card processing vendors, and three major U.S. credit reporting agencies.<sup>76</sup> According to Marriott, the company “furnished to the credit card networks all of the encrypted payment card data that was in the data tables [they] believe were involved in the incident, and the credit card networks then notified the banks that issued the cards.”<sup>77</sup>

---

<sup>73</sup> *Id.* at 4.

<sup>74</sup> *Id.*

<sup>75</sup> *Id.* at 4, 5.

<sup>76</sup> *Id.*

<sup>77</sup> Starwood Guest Reservation Database Security Incident Website, <https://answers.kroll.com/> (last accessed July 22, 2019).

189. As the investigation continued, the investigators found evidence that at some time between 2015 and 2016, the hackers created a copy of two *other* tables which were later deleted.<sup>78</sup> The file names correspond to two tables in the Starwood guest reservation database.<sup>79</sup> Marriott has been unable to recover those files and cannot determine what customer information in those tables was removed from the Starwood network.<sup>80</sup> Consequently, it is highly likely that additional data was stolen beyond what Marriott has already confirmed, including other Personal Information.

190. Accordingly, Marriott is still unable to provide consumers with a complete understanding or confirmation of the type of information stolen in the Data Breach. Marriott already verified that millions of customers' financial records were stolen, but numerous other Marriott customers provided personal financial data to Marriott during stays that was then subsequently utilized for fraud, identify theft, or otherwise misused, even though Marriott cannot confirm with certainty that such data was stolen in the breach. Given the incomplete nature of Marriott's records of what was stolen, Marriott's inability to confirm what data was exfiltrated, the nature of the hacking incident, and the type of data targeted, it is highly probable that additional unverified financial data was also exfiltrated during the four-year breach period.

191. The investigation revealed that customer information dating all the way back to 2002 was compromised in the breach, as well as customer information stored on Marriott's systems through September 10, 2018.

192. The following is a summary [REDACTED]  
[REDACTED]

---

<sup>78</sup> Sorenson Testimony at p. 4.

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

193. Marriott has subsequently acknowledged that it does not know the identity of the hackers and has not speculated as to the hackers' identities or their purpose for stealing this Personal Information.

*Marriott's Response to the Breach*

194. Although Marriott was on notice of a potential breach as early as September 8, 2018, it took Marriott **83** days to publicly acknowledge the breach and even longer to directly notify impacted customers via e-mail.

195. On November 30, 2018, Marriott publicly notified guests in a press release, stating that “there was unauthorized access to the database, which contained guest information relating to reservations at Starwood properties on or before September 10, 2018.”<sup>81</sup> Marriott initially reported that the Data Breach affected up to 500 million guests who made a reservation at a Starwood property,<sup>82</sup> including W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels, as well as Starwood-branded timeshare properties Sheraton Vacation Club, Westin Vacation Club, The Luxury Collection Residence Club, St. Regis Residence Club, and Vistana.

196. Marriott's announcement further stated that for approximately 327 million of the 500 million guests, the information compromised contained some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For the remaining guests, Marriott offered the opaque statement that

---

<sup>81</sup> *Marriott Announces Starwood Guest Reservation Database Security Incident* (hereinafter “Marriott Data Breach Announcement”), <https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/> (last accessed July 22, 2019).

<sup>82</sup> *Id.*

their “information was limited to name and sometimes other data such as mailing address, email address, or other information.”<sup>83</sup>

197. Marriott also said that for some guests, the information includes payment card numbers and payment card expiration dates, “but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128).” Marriott explained that “[t]here are two components needed to decrypt the payment card numbers,” but that it had “not been able to rule out the possibility that both were taken.”<sup>84</sup> In fact, evidence suggests hackers did take those components.

198. In the statement, Marriott CEO Arne Sorenson added: “We deeply regret this incident happened. We fell short of what our guests deserve and what we expect of ourselves. We are doing everything we can to support our guests, and using lessons learned to be better moving forward.”<sup>85</sup>

199. Following the November 30, 2018 press release, Marriott started sending email notifications to various guests who had valid email addresses in the compromised data tables. Marriott sent email notifications on a rolling basis, completing the email notice to domestic guests on December 11, 2018.

200. Marriott’s significant delay in notification was unreasonable, violated various state notification laws, and prevented impacted customers from taking immediate steps to protect themselves against identity theft and fraud. Indeed, due to Marriott’s delay, impacted customers were left with two choices: either wait for a full disclosure from Marriott before taking measures

---

<sup>83</sup> *Id.*

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*

to protect themselves, while risking identity theft and fraud; or take immediate mitigative measures to protect themselves against the risk of harm created by Marriott's inadequate security practices. Consumers would have been reasonable in making either choice.

201. Marriott's response to the breach, and the services it offered to consumers to address the breach, were insufficient and caused consumer confusion, resulting in consumers spending a significant amount of time taking measures to protect themselves—at Marriott's own repeated and widely dispersed recommendation. Thus, Marriott cannot be heard to complain about customers taking its advice and suggestions for how to respond in the face of the massive Data Breach.

202. Marriott's email notification procedure also raised concerns among security experts. To send the emails, Marriott created a separate domain—"email-marriott.com,"—which is registered to a third party firm on behalf of Marriott.<sup>86</sup> A major issue cited by technology reporters was that the email's sender domain does not look like a legitimate domain because the domain does not load to a website or have an identifying HTTPS certificate.<sup>87</sup> The email was also criticized for being "easily spoofable" (that is, easy for "cybersquatters" to mimic with similar-looking domains).<sup>88</sup> The FTC even warned consumers that "phishing scammers try to take advantage of situations like this" by "pos[ing] as legitimate companies and send[ing] emails with links to fake websites to try to trick people into sharing their personal information."<sup>89</sup>

---

<sup>86</sup> <https://www.cscglobal.com/service/dbs/digital-brand-services/> (last accessed July 22, 2019).

<sup>87</sup> Z. Whittaker, *Marriott's breach response is so bad, security experts are filling in the gaps—at their own expense*, TECHCRUNCH (Dec. 3, 2018), <https://techcrunch.com/2018/12/03/marriott-data-breach-response-risk-phishing/> (last accessed July 22, 2019).

<sup>88</sup> *Id.*

<sup>89</sup> S. Gressin, *The Marriott Data Breach*, FEDERAL TRADE COMMISSION, CONSUMER INFORMATION (Dec. 4, 2018), <https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach> (last accessed July 22, 2019).

203. The problems with Marriott’s email notifications were so apparent that two different cybersecurity experts registered similarly-named domains—“email-mariott.com” and “email-marriot.com”—to protect consumers from clicking on spoofed links. To the untrained eye, these look like legitimate domains – many would not notice the misspellings. The first was registered by Nick Carr who works for FireEye and the second belongs to Jake Williams, founder of Rendition Infosec.<sup>90</sup> In their words, “[h]ad Marriott just sent the email from its own domain, it wouldn’t be an issue.”<sup>91</sup>

204. Marriott also opened a call center and created a dedicated website—through a third-party company called Kroll—to answer questions about the Data Breach and provide access to a web monitoring service called WebWatcher. But the enrollment process for this service appeared to be intentionally camouflaged to prevent consumers from easily enrolling. For example, there was no link to “click here” or “enroll now” under the heading “Free WebWatcher Enrollment” on the announcement website. Instead, consumers were supposed to click on their country of origin *above* the announcement, even though there was no clear indication that the countries were “clickable” links.

205. Compounding this problem, the “FAQ” section of the website included a question entitled “*What is WebWatcher and how do I enroll?*” The corresponding answer stated that “WebWatcher monitors internet sites where personal information is shared and generates an alert if evidence of your personal information is found” – but failed to answer the question “*how do I enroll?*”

---

<sup>90</sup> Z. Whittaker, *Marriott’s breach response is so bad, security experts are filling in the gaps—at their own expense*, *supra* note 87.

<sup>91</sup> *Id.*

206. Additionally, the WebWatcher services offered by Marriott had obvious limitations. For one, critics decried the “relatively short [one year] window of coverage, since identity thieves often wait to use stolen data.”<sup>92</sup> Likewise, the service itself is not “particularly effective at protecting your data” because it is reactionary – it only alerts individuals *after* their information is located on underground websites.<sup>93</sup>

207. As noted by *Consumer Reports*, the WebWatcher service also does not include “a credit-monitoring service to alert consumers when new accounts have been opened in their name, which most identity theft services do include.”<sup>94</sup> Indeed, hallmarks of a robust monitoring product include not only “dark web” notifications, but also three-bureau credit monitoring, access to credit reports and credit scores, public record monitoring, bank and credit account takeover alerts, change of address alerts, access to an insurance policy, and access to agents who specialize in fraud resolution and identity restoration services. By depriving consumers of access to a more robust service, many affected individuals were unable to take necessary mitigative measures or were forced to pay out-of-pocket to protect themselves from Marriott’s security failures.

208. On January 4, 2019, Marriott issued a follow-up press release adjusting the number of affected records to 383 million guest records, including 23.75 million passport numbers (at least 5.25 million of which were unencrypted), and 9.1 million unique encrypted payment card numbers.<sup>95</sup> As of March 7, 2019, Marriott estimated that the information compromised “could

---

<sup>92</sup> O. Blanco, *Why Marriott’s ID Theft Protection May Not Be Enough*, CONSUMER REPORTS (Dec. 7, 2018), <https://www.consumerreports.org/identity-theft/why-marriotts-id-theft-protection-may-not-be-enough/> (last accessed July 22, 2019).

<sup>93</sup> *Id.*

<sup>94</sup> *Id.*

<sup>95</sup> Sorenson Testimony at p. 5.

include several thousand unencrypted payment card numbers.”<sup>96</sup> Marriott noted that investigators at that time had “not found evidence that the master encryption keys needed to decrypt encrypted payment card numbers were accessed” – but could not rule out that possibility (and experts view it as likely having occurred). Thus, even though 9.1 million payment card numbers were encrypted, it is likely that the hackers had access to the full payment card information with encryption keys.

209. During the time between discovery of the Data Breach and Marriott’s retiring of the Starwood database, Marriott reportedly took measures to secure the Starwood network, including “malware removal, deployment of endpoint protection tools to approximately 70,000 devices that were originally on the Starwood network, rebuilding impacted hosts, and IP whitelisting to control access to the Starwood database.”<sup>97</sup> Marriott reportedly retired its use of the Starwood guest reservation database for business operations as of December 18, 2018.<sup>98</sup>

#### ***Reactions to the Breach and Government and Regulatory Investigations***

210. Reactions to the Data Breach from industry security analysts and Congressional members highlight its severity. Chris Wysopal, chief technology officer of security company Veracode, stated that: “On a scale of 1 to 10 and up, this is one of those No. 10 size breaches. There have only been a few of them of this scale and scope in the last decade.”<sup>99</sup>

211. Ollie Whitehouse, Global Chief Technology Officer at IT security company NCC Group, stated that: “Marriott Hotels should have identified this breach through their cyber due diligence of Starwood in 2016 when it acquired the company. As result of buying a breach they

---

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> *Id.*

<sup>99</sup> Democrat-Gazette Staff Wire Reports, *Breach Puts Hotel Guests’ Data at Risk*, ARKANSAS DEMOCRAT GAZETTE (Dec. 1, 2018), <https://www.arkansasonline.com/news/2018/dec/01/breach-puts-hotel-guests-data-at-risk-2/> (last accessed July 22, 2019).

will face a number of challenges at a board level around the levels of governance and diligence within the business. Had it performed a detailed compromise assessment as part of its due-diligence activity, the organization's board would have been informed of the breach and been able to make a decision based on risk or put other warranties in place.”<sup>100</sup>

212. Joseph Carson, Chief Security Scientist at security company Thycotic, stated that: “What is shocking about this data breach is that the cybercriminals potentially got away with both the encrypted data as well as the methods to decrypt the data which appears that Marriott have not practiced adequate cybersecurity protection for their customers personal and sensitive information.”<sup>101</sup>

213. Satya Gupta, Global Chief Technology Officer and Co-Founder of cyber-security company Virsec, stated that: “What's most disturbing about this attack is the enormous dwell time inside Starwood's systems. The attackers apparently had unauthorized access since 2014 – a massive window of opportunity to explore internal servers, escalate privileges, move laterally to other systems, and plot a careful exfiltration strategy before being discovered. All organizations should assume that the next threat is already inside their networks and won't be caught by conventional perimeter security. We need much more careful scrutiny of what critical applications are actually doing to spot signs of internal corruption. We must reduce dwell time from years to seconds.”<sup>102</sup>

---

<sup>100</sup> M. Zorz, *Industry Reactions to the Enormous Marriott Data Breach*, HELPNET SECURITY (Nov. 30, 2018), <https://www.helpnetsecurity.com/2018/11/30/marriott-data-breach-reactions/> (last accessed July 22, 2019).

<sup>101</sup> *Id.*

<sup>102</sup> *Security Experts, Industry Leaders Reaction on Marriott Data Breach Exposing 500M Customers*, ISBUZZ NEWS (Dec. 3, 2018), <https://www.informationsecuritybuzz.com/expert-comments/marriott-data-breach/> (last accessed July 22, 2019).

214. Matt Walmsley, EMEA Director at Vectra, stated that: “This breach also demonstrates that incident response continues to take too long, and in many cases the result is security teams trying to figure out ‘what just happened, how do we stop it happening again?’ rather than spotting, understanding and closing down an attacker earlier in its lifecycle to minimi[ze] or stop a breach occurring.”<sup>103</sup>

215. Tom van de Wiele, a security consultant at cybersecurity and privacy company F-Secure, stated that: “The most disappointing part of this hack is the fact that the amount of data stolen is one of the bigger ones of the last few years and further made worse by the fact that the compromise had been going on for at least four years according to several online publications. This indicates that as far as security monitoring and being able to respond in a timely and adequate fashion, Marriott had severe challenges being able to live up to its mission statement of keeping customer data safe.”<sup>104</sup>

216. Marriott has also been condemned by members of Congress who faulted Marriott for moving too slowly to phase out Starwood’s software. For example, on March 7, 2019, the U.S. Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations held a hearing on “Examining Private Sector Data Breaches” and lawmakers admonished Marriott for its deficient data security practices. In particular, Democratic Sen. Jacky Rosen (Nev.), who

---

<sup>103</sup> M. Zorz, *Industry Reactions to the Enormous Marriott Data Breach*, *supra* note 100.

<sup>104</sup> *Id.*

previously worked in IT, expressed surprise that Marriott had taken “no method of auditing the data coming across” following its acquisition of Starwood.<sup>105</sup>

217. On November 30, 2018, Texas Attorney General Ken Paxton announced that his office served an investigative subpoena on Marriott, seeking documents and other information to examine the nature and extent of this data breach. The state Attorneys General for New York, Massachusetts, Illinois, Connecticut, Maryland, and Pennsylvania have also indicated they are investigating the Data Breach.

218. In the European Union, the Information Commissioner’s Office (“ICO”) is leading an investigation into the Data Breach. Marriott is subject to the European Union’s General Data Protection Regulation (“GDPR”), which became effective in May 2018, and various U.S. state and federal laws governing the protection of personal information and data privacy. Specifically, the GDPR imposes compliance obligations for handling of personal information and has increased financial penalties for noncompliance – “monetary penalties of up to 4% of worldwide revenue.”

219. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

<sup>106</sup>

---

<sup>105</sup> A. Gregg, *The Cybersecurity 202: Senators Call for Data Breach Penalties, Tougher Privacy Laws After Marriott Hack*, THE WASHINGTON POST (Dec. 3, 2018), <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/12/03/the-cybersecurity-202-senators-call-for-data-breach-penalties-tougher-privacy-laws-after-marriott-hack/5c0436431b326b60d12800d2/> (last accessed July 22, 2019).

<sup>106</sup> [REDACTED]

220. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>107</sup>

221. On July 9, 2019, the ICO issued a “notice of intention to fine” Marriott £99 million (\$123 million) for violations of the GDPR. The ICO concluded that Marriott failed to conduct sufficient due diligence when it acquired Starwood and should have done more to ensure the Starwood systems were secure, in violation of the GDPR.<sup>108</sup>

222. In a statement, ICO commissioner Elizabeth Denham stated: “The GDPR makes it clear that organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected. Personal data has a real value so organizations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn’t happen, we will not hesitate to take strong action when necessary to protect the rights of the public.”<sup>109</sup>

223. Immediately following imposition of the penalty, Marriott stated its intention to contest the fine: “We are disappointed with this notice of intent from the ICO, which we will contest,” said Marriott CEO Arne Sorenson. “Marriott has been cooperating with the ICO

---

<sup>107</sup> [REDACTED]

<sup>108</sup> ICO News, *Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach*, (July 9, 2019), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/> (last accessed July 22, 2019).

<sup>109</sup> *Id.*

throughout its investigation into the incident, which involved a criminal attack against the Starwood guest reservation database. We deeply regret this incident happened.”<sup>110</sup>

***An Independent Report Confirms Marriott’s Deficient Data Security Practices***

224. The Payment Card Industry Data Security Standard (“PCI DSS”) “is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.”<sup>111</sup> The standards are intended to protect the sensitive information involved in processing payments.<sup>112</sup> The PCI Security Standards Council (“PCI SSC”) was launched in September 2006 in an effort to manage the ongoing evolution of the PCI security standards with a focus on improving payment account security throughout the transaction process.<sup>113</sup>

225. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]  
[REDACTED]  
[REDACTED]

b. [REDACTED]  
[REDACTED]  
[REDACTED]

---

<sup>110</sup> <https://news.marriott.com/2019/07/marriott-international-update-on-starwood-reservation-database-security-incident/> (last accessed July 22, 2019).

<sup>111</sup> PCI FAQ, <https://www.pcicomplianceguide.org/faq/#1> (last accessed July 22, 2019).

<sup>112</sup> *Marriott Data Security Breach Lessons: Why PCI Levels Matter*, PDC FLOW (Dec. 18, 2018), <https://www.pdcflow.com/payment-compliance/marriott-data-security-breach-lessons-why-pci-compliance-levels-matter/> (last accessed July 22, 2019).

<sup>113</sup> PCI FAQ, *supra* note 111.

c. [REDACTED]  
[REDACTED]  
[REDACTED]

d. [REDACTED]  
[REDACTED]  
[REDACTED]

e. [REDACTED]  
[REDACTED]

226. [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

227. A company with proper information security would not have allowed outsiders to have access to such a massive variety of information systems over four years even if they somehow managed to access internal systems for a brief period of time. [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

228. [REDACTED]

[REDACTED]

[REDACTED]

229. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

230. Moreover, for at least four years, [REDACTED]

[REDACTED]

[REDACTED]

231. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

232. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

233. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

234. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] it is highly probable that at least one or more threat actors had already accessed, exfiltrated the files containing encrypted cardholder values, and ascertained how to decrypt the files. Once one card was decrypted successfully, the process of writing a script to do so for the entire database would have been simple. [REDACTED]

it would have been completely undetectable. Moreover, several databases that were created by the

hackers were deleted and Marriott has suggested that it cannot confirm what data was in those files.

235. Marriott's post-breach response was also lacking. It implemented infrastructure changes after discovering the breach that only changed known compromised devices and credentials, even though [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Starwood should have assumed that hackers still had access to its systems and ensured that all of its systems were clean before redeploying the systems again.

236. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

237. It is also highly unlikely that every malicious actor left evidence of their activity. Therefore, it is highly probable that there were more intrusions; the evidence was either wiped by

the attacker or was unable to be uncovered four years later due to the passage of time and degradation of digital evidence.

238. [REDACTED]

[REDACTED] It is highly plausible that at least some of these attacks were from different hackers [REDACTED] because such attacks would otherwise be redundant.

239. [REDACTED]

240. [REDACTED]

[REDACTED] It is proper industry practice to assume that all accounts were compromised (because of infiltration of what are known as active directory and domain controllers). For this reason, Marriott should be ordered to wipe and redeploy all legacy Starwood systems whenever possible and isolate (and rebuild and reimage) whenever it is not. Additionally, Marriott should be ordered to reset all accounts and properly secure administrative access.

***Accenture's Role in the Data Breach***

241. Accenture describes itself as “one of the world’s leading professional service companies” and provides a range of services including management and technology consulting

services. Accenture represents clients in 120 countries and reported net revenues of nearly \$40 billion in 2018.

242. In 2009, Accenture and Starwood entered into a \$200 million contract to outsource the maintenance of Starwood's IT and security infrastructure to Accenture. Accenture's services included "development, testing, maintenance and running of the applications. Infrastructure outsourcing services include server and storage management, data center management, end-user computing, network management and service desk management."<sup>114</sup>

243. Marriott likewise transferred its finance and accounting services to Accenture in 2013 after previously handling those services in-house. As part of a 10-year agreement, Accenture collaborated in managing Marriott's finance and accounting operations with Marriott Business Services, a wholly-owned subsidiary of Marriott.

244. [REDACTED]

[REDACTED]<sup>115</sup>

245. [REDACTED]

[REDACTED]<sup>116</sup>

246. [REDACTED]

---

<sup>114</sup> J. Bosavage, *Accenture Books \$200 Million Deal with Starwood*, CRN (Mar. 15, 2010), <https://www.crn.com/news/channel-programs/223800264/accenture-books-200-million-deal-with-starwood.htm> (last accessed July 22, 2019).

<sup>115</sup> [REDACTED]

<sup>116</sup> [REDACTED]

[REDACTED]

[REDACTED]<sup>117</sup>

247. Following the announcement of the Marriott and Starwood merger, Accenture continued to provide services to Starwood and Marriott including facilities, personnel, software and equipment and other resources necessary to the security of the application, infrastructure, and security domains. In particular, [REDACTED]

[REDACTED]<sup>118</sup>

248. Following the acquisition, Marriott hosted the Starwood guest reservation database on Marriott-owned hardware in a data center operated by Digital Realty in Phoenix, Arizona. Accenture continued managing the operation of the Starwood guest reservation database, as it had since late 2009.

249. At all relevant times, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>119</sup> [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>117</sup> [REDACTED].

<sup>118</sup> [REDACTED]

<sup>119</sup> [REDACTED].

250. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

251. In describing Accenture's role, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>120</sup>

252. Accenture knew the information stored on the Starwood database contained valuable, sensitive information of Starwood guests and was specifically tasked with identifying security threats in order to prevent unauthorized access of Starwood's systems.

253. As described herein, Accenture repeatedly failed over a four-year period to identify critical security threats such as unauthorized queries on Starwood's guest reservation database and malware specifically designed to access and exfiltrate sensitive information.

254. Accenture recognized that its failure to adequately secure its clients' systems could result in significant harm to its clients and jeopardize its own business operations. As noted in a recent public filing:

In providing services and solutions to clients, we often manage, utilize and store sensitive or confidential client or Accenture data, including personal data, and we

---

<sup>120</sup> [REDACTED]

expect these activities to increase, including through the use of artificial intelligence, the internet of things and analytics. Unauthorized disclosure of sensitive or confidential client or Accenture data, whether through systems failure, employee negligence, fraud, misappropriation, or other intentional or unintentional acts, could damage our reputation, cause us to lose clients and could result in significant financial exposure. Similarly, unauthorized access to or through our or our service providers' information systems or those we develop for our clients, whether by our employees or third parties, including a cyberattack by computer programmers, hackers, members of organized crime and/or state-sponsored organizations, who continuously develop and deploy viruses, ransomware or other malicious software programs or social engineering attack, could result in negative publicity, significant remediation costs, legal liability, damage to our reputation and government sanctions and could have a material adverse effect on our results of operations.<sup>121</sup>

255. In conjunction with Starwood and Marriott, Accenture's ongoing failure to maintain adequate security controls to detect and neutralize known and obvious security threats over a four-year period was a direct and proximate cause of the Data Breach.

***Marriott Failed to Comply with Regulatory Guidance***

256. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.<sup>122</sup>

257. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and

---

<sup>121</sup> Accenture U.S. SEC 2018 Form 10-K at 11, <https://www.accenture.com/acnmedia/PDF-89/Accenture-2018-10-K.pdf> (last accessed July 22, 2019).

<sup>122</sup> Federal Trade Commission, *Start With Security* (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed July 22, 2019).

practices for business.<sup>123</sup> Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>124</sup>

258. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.<sup>125</sup>

259. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.<sup>126</sup>

---

<sup>123</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed July 22, 2019).

<sup>124</sup> *Id.*

<sup>125</sup> FTC, *Start With Security*, *supra* note 122.

<sup>126</sup> Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last accessed July 22, 2019).

260. In this case, Marriott was fully aware of its obligation to use reasonable measures to protect the personal information of its customers, acknowledging as much in its own privacy policies. Marriott also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Marriott failed to comply with industry-standard data security requirements.

261. Marriott's failure to employ reasonable and appropriate measures to protect against unauthorized access to its customers' information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

***The Effect of the Data Breach on Impacted Consumers***

262. Given the sensitive nature of the Personal Information stolen in the Data Breach—including names, mailing addresses, email addresses, phone numbers, passport numbers, dates of birth, and travel information (and likely other sensitive information that was unable to be confirmed)—hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and class members now and into the indefinite future and have already done so.

263. In fact, many victims of the Data Breach have already experienced significant harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, and fraudulent payment card purchases. Plaintiffs and class members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, replacing passports, checking credit reports, and spending time and effort searching for unauthorized activity.

264. The Personal Information exposed in the Data Breach is highly-coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which

criminals openly post and sell stolen consumer information on underground internet websites known as the “dark web” – exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver’s license or ID card in the victim’s name; (e) obtain fraudulent government benefits or medical treatment; (f) file a fraudulent tax return using the victim’s information; (g) commit passport fraud; (h) commit espionage; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

265. Additionally, victims of the Data Breach are at risk of harm unique to this breach, including having their guest reward points siphoned for misuse. For example, *Bloomberg* notes that: “Hackers have found it’s increasingly easy to access rewards portals and quickly redeem consumers’ hard-earned points and miles for gift cards or hotel stays.”<sup>127</sup> In fact, “data associated with these programs has become increasingly valuable to criminals: on the dark web, a consumer’s Social Security number often sells for \$1, while loyalty-account information can fetch 20 times that.”<sup>128</sup>

266. Victims who had their passport numbers compromised are at an even greater risk of harm. Hackers can combine exposed passport numbers with other personal information to create false identities or fraudulent passports, which are “often linked to illegal immigration, contraband

---

<sup>127</sup> J. Surane & K. Chiglinsky, *All Those Starwood Points You Racked Up at Risk in Marriott Hack*, BLOOMBERG (Nov. 30, 2018), <https://www.bloomberg.com/news/articles/2018-11-30/all-those-starwood-points-you-racked-up-at-risk-in-marriott-hack> (last accessed July 22, 2019).

<sup>128</sup> *Id.*

smuggling, economic crimes, international terrorism and other serious crimes.”<sup>129</sup> According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding passport fraud:

Fraudulent passports pose a significant risk because they can be used to conceal the true identity of the user. In addition, according to the Department of State (State), passport and visa fraud are often committed in connection with crimes such as international terrorism, drug trafficking, organized crime, alien smuggling, money laundering, pedophilia, and murder. As a result, even a few instances of passport fraud can have far-reaching effects.<sup>130</sup>

267. For this reason, passport information is a valuable commodity on underground markets, especially when it is paired with other data points tied to an individual such as those exposed by Marriott here. As noted by Brian Stack, vice president of dark web intelligence at Experian: “Knowing this passport number is tied to an individual is valuable.”<sup>131</sup> This is because “[c]riminals can use your passport number, along with your name and several other points of data that were in Marriott’s database for customers of its Starwood division, to impersonate you online. They could also use the number to create a more authentic forgery, something that could be worth thousands of dollars on the black market.”<sup>132</sup>

268. For victims who opt to replace their passports, the multi-step process is time consuming and costly. First, individuals must report the loss to the U.S. State Department so that the passport will be invalidated and cannot be used for travel. This requires filling out a Form DS-

---

<sup>129</sup> <https://www.us-passport-service-guide.com/passport-fraud.html> (last accessed July 22, 2019).

<sup>130</sup> U.S. Government Accountability Office Report to Congressional Requesters, *Pervasive Passport Fraud Not Identified, but Cases of Potentially Fraudulent and High-Risk Issuances Are under Review* (May 2014), <https://www.gao.gov/assets/670/662921.pdf> (last accessed July 22, 2019).

<sup>131</sup> L. Hautala, *Marriott Breach: What to do when hackers steal your passport number*, CNET (Dec. 3, 2018), <https://www.cnet.com/news/marriott-breach-what-to-do-when-hackers-steal-your-passport-number/> (last accessed July 22, 2019).

<sup>132</sup> *Id.*

64, which requires an explanation of how the passport was lost or stolen and requires the submission of the identifying information of the passport-holder including full name, address, place of birth, and Social Security number, among other personal information.

269. Next, the victim must get new passport photos taken, which typically cost \$15 or more at the U.S. Post Office. The applicant then has to travel in-person to a passport acceptance facility to apply for a new passport. This requires providing a copy of a U.S. birth certificate or certificate of naturalization or citizenship, a government-issued photo ID, and the new passport photos. The cost of obtaining a new passport is \$140 for a passport book and card, plus an additional \$35 acceptance fee to obtain the passport through an authorized passport acceptance facility. The applicant must then wait weeks or even months for the new passport to arrive.

270. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- a. purchasing goods and services they would not have otherwise paid for and/or paying more for good and services than they otherwise would have paid, had they known the truth about Defendants' substandard data security practices;
- b. losing the inherent value of their Personal Information;
- c. losing the value of the explicit and implicit promises of data security;
- d. identity theft and fraud resulting from the theft of their Personal Information;
- e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;
- g. costs associated with replacing passports or addressing passport-related fraud;
- h. loss of value of reward points accumulated through the purchase of goods or services;

- i. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- j. lowered credit scores resulting from credit inquiries following fraudulent activities;
- k. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and
- l. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

271. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.<sup>133</sup>

272. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

---

<sup>133</sup> E. Harrell, U.S. Department of Justice, *Victims of Identity Theft*, 2014 (revised Nov. 13, 2017), <http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last accessed July 22, 2019).

continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>134</sup>

273. Plaintiffs and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.<sup>135</sup>

274. The cost of purchasing a hotel room includes tangible and intangible components, including things such as the overall cost of the property and employee costs, as well the cost of providing conveniences like soaps and shampoos. One component of the cost of a hotel room is the explicit and implicit promises Marriott made to protect its customers' Personal Information. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Marriott and Starwood would have no reason to tout their data security efforts to their actual and potential customers.

275. Consequently, had consumers known the truth about Defendants' data security practices—that they did not adequately protect and store their data—they would not have stayed at a Marriott Property, purchased products or services at a Marriott Property, and/or would have

---

<sup>134</sup> U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), <http://www.gao.gov/new.items/d07737.pdf> (last accessed July 22, 2019).

<sup>135</sup> FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), [https://www.fireeye.com/blog/executive-perspective/2016/05/beyond\\_the\\_bottomli.html](https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html) (last accessed July 22, 2019).

paid less. As such, Plaintiffs and class members did not receive the benefit of their bargain with Defendants because they paid for the value of services they expected but did not receive.

### **CLASS ACTION ALLEGATIONS**

#### **NATIONWIDE CLASS**

276. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the “Nationwide Class” or the “Class”

**All natural persons residing in the United States whose Personal Information was compromised in the Data Breach.**

277. The Nationwide Class asserts claims against Marriott and Starwood for negligence (Count 1), negligence *per se* (Count 2), breach of contract (Count 3), breach of implied contract (Count 4), unjust enrichment (Count 5), declaratory judgment (Count 6), violations of the Maryland Personal Information Protection Act, Md. Comm. Code §§ 14-3501, *et seq.*, (Count 7); and violations of the Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-301, *et seq.* (Count 8). The Nationwide Class also asserts claims against Accenture for negligence (Count 95), and negligence *per se* (Count 96). All causes of action asserted below are against Marriott and Starwood except where otherwise indicated.

#### **STATEWIDE [NAME OF STATE OR TERRITORY] SUBCLASS**

278. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 9 through 94), on behalf of separate statewide subclasses for each State, the District of Columbia, Puerto Rico, and the Virgin Islands (the “Statewide Subclasses”), defined as follows:

**All natural persons residing in [name of state or territory] whose Personal Information was compromised in the Data Breach.**

279. Excluded from the Nationwide Class and each Statewide Subclass are Marriott and Accenture, any entity in which Marriott or Accenture has a controlling interest, and Marriott's and Accenture's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Statewide Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

280. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all class members is impracticable. While the exact number of class members is unknown to Plaintiffs at this time, Marriott has acknowledged that Personal Information of hundreds of millions of its customers has been compromised. Those individuals' names and addresses are available from Marriott's records, and class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. Indeed, Marriott has stated that it has already provided direct notice of the breach to class members. On information and belief, there are at least thousands of class members in each Statewide Subclass, making joinder of all Statewide Subclass members impracticable.

281. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** As to the Nationwide Class and each Statewide Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual class members, including, but not limited to, the following:

- a. Whether Marriott knew or should have known that its computer systems were vulnerable to attack;

- b. Whether Marriott and/or Accenture failed to take adequate and reasonable measures to ensure Marriott's data systems were protected;
- c. Whether Marriott and/or Accenture failed to take available steps to prevent and stop the breach from happening;
- d. Whether Marriott failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard its customers' Personal Information;
- e. Whether Marriott failed to provide timely and adequate notice of the data breach;
- f. Whether Marriott and/or Accenture owed a duty to Plaintiffs and class members to protect their Personal Information and to provide timely and accurate notice of the data breach to Plaintiffs and class members;
- g. Whether Marriott and/or Accenture breached their duties to protect the Personal Information of Plaintiffs and class members by failing to provide adequate data security and by failing to provide timely and accurate notice to Plaintiffs and class members of the data breach;
- h. Whether Marriott and/or Accenture's conduct, including their failure to act, resulted in or was the proximate cause of the breach of Marriott's systems, resulting in the unauthorized access to and/or theft of its customers' Personal Information;
- i. Whether Marriott has a contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;
- j. Whether Marriott's conduct amounted to violations of state consumer protection statutes, and/or state data breach statutes;

- k. Whether, as a result of Defendants' conduct, Plaintiffs and Class and Subclass members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and
- l. Whether, as a result of Defendants' conduct, Plaintiffs and Class and Subclass members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

282. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Nationwide Class and each Statewide Subclass, Plaintiffs' claims are typical of other class members' claims because Plaintiffs and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

283. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate class representatives because their interests do not conflict with the interests of class members who they seek to represent, Plaintiffs have retained counsel competent and experienced in complex class action litigation and data breach litigation, and Plaintiffs intend to prosecute this action vigorously. The class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

284. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).** The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Defendants. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other class members and impair their interests. Defendants have acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

285. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for class members to individually seek redress for Defendants' wrongful conduct.

#### **CHOICE OF LAW FOR NATIONWIDE CLAIMS**

286. The state laws of one state will likely govern Plaintiffs' claims.

287. First, the principal place of business of Marriott, located in Bethesda, Maryland, is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

288. Alternatively, the former principal place of business of Starwood, Stamford, Connecticut, was the center of operations of Starwood and its SPG Loyalty Program, and the place where, on information and belief, its high-level officers directed, controlled, and coordinated the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

289. Both Maryland and Connecticut have significant interests in regulating the conduct of businesses operating within their borders. Those states, which seek to protect the rights and interests of residents and citizens of the United States against a company headquartered and doing business in those states, have a greater interest in the nationwide claims of Plaintiffs and class members than any other state and are most intimately concerned with the claims and outcome of this litigation.

290. Marriott's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in Maryland.

291. Marriott's breaches of duty to Plaintiffs and Nationwide Class members emanated from both Connecticut and Maryland.

292. Additional factual analysis is necessary in order to determine which state's law should apply to the claims of the class members. Accordingly, it would be inappropriate to determine choice of law at the pleadings stage of this case. Plaintiffs are therefore pleading nationwide claims based upon Maryland and Connecticut law in the alternative (or under the law of the states of each Plaintiff).

293. Application of either Maryland or Connecticut law with respect to Plaintiffs' and class members' claims after the completion of a factual inquiry would be neither arbitrary nor fundamentally unfair because those states have significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and class members.

294. Under choice of law principles applicable to this action, the common law of one of the states—Maryland or Connecticut—would apply to the nationwide common law claims of all class members given Maryland's and Connecticut's significant interest in regulating the conduct of businesses operating within their borders, consumer protection laws may be applied to non-resident consumer plaintiffs upon completion of the factual analysis required for the choice of law determination.

295. To the extent the Court finds that the laws of each Class member's state apply to his or her injuries, Plaintiffs previously provided Marriott with notice sufficient to satisfy state statutory requirements, and sent correspondence to Marriott's counsel on January 8, 2019, providing the company with additional information on Plaintiffs' claim.

**CLAIMS ON BEHALF OF THE NATIONWIDE CLASS  
AGAINST MARRIOTT AND STARWOOD**

**COUNT 1**

**NEGLIGENCE**

**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs  
and the Statewide Subclasses**

296. Plaintiffs repeat and allege Paragraphs 1-295, as if fully alleged herein.

297. Marriott owed a duty to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Marriott's security systems to ensure that Plaintiffs' and class members' Personal Information in Marriott's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

298. Marriott had a common law duty to prevent foreseeable harm to its customers. This duty existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, Marriott knew that it was more likely than not Plaintiffs and other class members would be harmed.

299. Marriott's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . .

practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Marriott. Various FTC publications and data security breach orders further form the basis of Marriott’s duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

300. Marriott also had a duty to safeguard the Personal Information of Plaintiffs and class members and to promptly notify them of a breach because of state laws and statutes that require Marriott to reasonably safeguard Personal Information, as detailed herein.

301. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiffs and class members could take appropriate measures to freeze or lock their credit profiles, cancel current passports and obtain new passports, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Marriott’s misconduct.

302. Marriott breached the duties it owed to Plaintiffs and class members described above and thus was negligent. Marriott breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiffs and class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose in a timely fashion that Plaintiffs’ and the class members’ Personal Information in Marriott’s possession had been or was reasonably believed to have been, stolen or compromised.

303. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiffs and class members, their Personal Information would not have been compromised.

304. As a direct and proximate result of Marriott's negligence, Plaintiffs and class members have been injured as described herein, and are entitled to damages in an amount to be proven at trial. Plaintiffs and class members injuries include, but are not limited to, the following:

- a. purchasing goods and services they would not have otherwise paid for and/or paying more for good and services than they otherwise would have paid, had they known the truth about Marriott's substandard data security practices;
- b. losing the inherent value of their Personal Information;
- c. losing the value of the explicit and implicit promises of data security;
- d. identity theft and fraud resulting from the theft of their Personal Information;
- e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;
- g. costs associated with replacing passports or addressing passport-related fraud;
- h. loss of value of reward points accumulated through the purchase of goods or services;
- i. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- j. lowered credit scores resulting from credit inquiries following fraudulent activities;

- k. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and
- l. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

## **COUNT 2**

### **NEGLIGENCE *PER SE***

#### **On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

305. Plaintiffs repeat and allege Paragraphs 1-295, as if fully alleged herein.

306. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair act or practice by companies such as Marriott of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Marriott’s duty.

307. Marriott violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry standards. Marriott’s conduct was particularly unreasonable given the nature and amount of

Personal Information it obtained and stored and the foreseeable consequences of a data breach on its systems.

308. Marriott's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

309. Nationwide Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

310. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and class members.

311. As a direct and proximate result of Marriott's negligence, Plaintiffs and Class members have been injured as described herein, and are entitled to damages in an amount to be proven at trial.

### **COUNT 3**

#### **BREACH OF CONTRACT**

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

312. Plaintiffs repeat and allege Paragraphs 1-295, as if fully alleged herein.

313. Marriott's Privacy Statement is an agreement between Marriott and individuals who provided their Personal Information to Marriott, including Plaintiffs and class members.

314. Marriott's Privacy Statement states that individuals are subject to its terms and conditions when they perform any of the following acts: (1) log onto Marriott's website; (2) use Marriott's software applications; (3) access Marriott's social media pages; (4) receive e-mail

communications from Marriott that link to the Privacy Statement; and (5) “when you visit or stay as a guest at one of our properties, or through other offline interactions.” Marriott’s Privacy Statement provides that: “Collectively, we refer to the Websites, the Apps and our Social Media Pages, as the ‘Online Services’ and, together with offline channels, the ‘Services.’ ***By using the Services, you agree to the terms and conditions of this Privacy Statement.***” (emphasis added).

315. Likewise, the terms and conditions governing the Marriott Rewards Program state that: “By opening a Membership Rewards Program account ... You consent to the Company’s processing of data that is personal to You, and disclosure of such data to third parties, in accordance with the Company’s privacy statement.”

316. Plaintiffs and class members provided their Personal Information to Marriott when they, among other things, used Marriott’s services, enrolled in Marriott’s Reward Program, purchased products and services from Marriott, and/or booked reservations at a Marriott Property via offline and online channels. Consequently, Plaintiffs and class members who transacted with Marriott manifested their willingness to enter into a bargain with Marriott and intention to assent to the terms of the Privacy Statement by providing their Personal Information to Marriott.

317. Conversely, Marriott, in collecting Plaintiffs’ and class members’ Personal Information, manifested its intent to adhere to its obligations under the Privacy Statement, including using “reasonable organizational, technical and administrative measures to protect [its customers’] Personal Data.”

318. Likewise, Starwood’s online Privacy Statement dated October 14, 2014 is an agreement between Starwood and individuals who provided their Personal Information to Starwood, including Plaintiffs and class members.

319. Starwood's Privacy Statement provides that Starwood collects individuals' Personal Information when they, among other things: (1) make reservations or submit information requests to Starwood; (2) purchase products or services from Starwood; (3) register for Starwood program membership; and (4) respond to communications from Starwood.

320. Starwood's Privacy Statement also sets forth Starwood's obligations to protect the customer information it collects, including that "Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your PII against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control."

321. Starwood's Privacy Statement provides a detailed list of specific groups with which it will share its customers' Personal Information and under what circumstances. It also promises that it "safeguard[s] your information using appropriate administrative, procedural and technical safeguards, including password controls, 'firewalls' and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit."

322. Likewise, the terms and conditions governing the SPG Program state that: "By becoming a member of the SPG Program (an 'SPG Member') and receiving and redeeming benefits of the SPG Program including, without limitation, Starpoints®, each SPG Member agrees that he/she has ... provided consent for Starwood, the SPG Participating Hotels and their authorized third party agents to process data that is personal to him/her, and to disclose such data to third parties, in accordance with Starwood's Privacy Statement."

323. Plaintiffs and class members provided their Personal Information to Starwood when they, among other things, used Starwood's services, enrolled in the SPG Program, purchased products and services from Starwood, and/or booked reservations at a Starwood property via offline and online channels. Consequently, Plaintiffs and class members who transacted with Starwood manifested their willingness to enter into a bargain with Starwood and intention to assent to the terms of the Privacy Statement by providing their Personal Information to Starwood.

324. Conversely, Starwood, in collecting Plaintiffs' and class members' Personal Information, manifested its intent to adhere to its obligations under the Privacy Statement, including "hav[ing] security measures in place to help protect [customers'] PII against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under [Starwood's] control."

325. Plaintiffs and class members on the one hand and Marriott and Starwood on the other formed contracts when Plaintiffs and class members provided Personal Information to Marriott and Starwood subject to their Privacy Statements.

326. Plaintiffs and class members fully performed their obligations under the contracts with Marriott and Starwood.

327. Marriott and Starwood breached their agreements with Plaintiffs and class members by failing to protect their Personal Information. Specifically, Marriott and Starwood (1) failed to use reasonable organizational, technical, procedural, and administrative measures to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of their agreements.

328. As a direct and proximate result of these breaches of contract, Plaintiffs and class members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

#### **COUNT 4**

#### **BREACH OF IMPLIED CONTRACT**

##### **On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

329. Plaintiffs repeat and allege Paragraphs 1-295, as if fully alleged herein, and assert this claim in the alternative to their breach of contract claim to the extent necessary.

330. Plaintiffs and class members also entered into an implied contract with Marriott when they obtained services from Marriott, or otherwise provided Personal Information to Marriott.

331. As part of these transactions, Marriott agreed to safeguard and protect the Personal Information of Plaintiffs and class members and to timely and accurately notify them if their Personal Information was breached or compromised.

332. Plaintiffs and class members entered into the implied contracts with the reasonable expectation that Marriott's data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and class members believed that Marriott would use part of the monies paid to Marriott under the implied contracts to fund adequate and reasonable data security practices.

333. Plaintiffs and class members would not have provided and entrusted their Personal Information to Marriott or would have paid less for Marriott's services in the absence of the implied contract or implied terms between them and Marriott. The safeguarding of the Personal

Information of Plaintiffs and class members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

334. Plaintiffs and class members fully performed their obligations under the implied contracts with Marriott.

335. Marriott breached its implied contracts with Plaintiffs and class members to protect their Personal Information when it (1) failed to have security protocols and measures in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their Personal Information was compromised as a result of the data breach.

336. As a direct and proximate result of Marriott's breaches of implied contract, Plaintiffs and class members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

### **COUNT 5**

#### **UNJUST ENRICHMENT**

**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

337. Plaintiffs repeat and allege Paragraphs 1-295, as if fully alleged herein, and assert this claim in the alternative to their breach of contract claims to the extent necessary.

338. Plaintiffs and class members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Marriott and that was ultimately stolen in the Data Breach.

339. Marriott was benefitted by the conferral upon it of the Personal Information pertaining to Plaintiffs and class members and by its ability to retain and use that information. Marriott understood that it was in fact so benefitted.

340. Marriott also understood and appreciated that the Personal Information pertaining to Plaintiffs and class members was private and confidential and its value depended upon Marriott maintaining the privacy and confidentiality of that Personal Information.

341. But for Marriott's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with Marriott. Further, if Marriott had disclosed that its data security measures were inadequate, Marriott would not have been permitted to continue in operation by regulators, its shareholders, and its customers.

342. As a result of Marriott's wrongful conduct as alleged in this Complaint (including, among things, its knowing failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiffs and class members without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), Marriott has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members. Marriott continues to benefit and profit from its retention and use of the Personal Information while its value to Plaintiffs and class members has been diminished.

343. Marriott's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and class members' Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

344. Under the common law doctrine of unjust enrichment, it is inequitable for Marriott to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and class members in an unfair and unconscionable manner. Marriott's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

345. The benefit conferred upon, received, and enjoyed by Marriott was not conferred officiously or gratuitously, and it would be inequitable and unjust for Marriott to retain the benefit.

346. Marriott is therefore liable to Plaintiffs and class members for restitution in the amount of the benefit conferred on Marriott as a result of its wrongful conduct, including specifically the value to Marriott of the Personal Information that was stolen in the Data Breach and the profits Marriott is receiving from the use of that information.

### **COUNT 6**

### **DECLARATORY JUDGMENT**

#### **On Behalf of Plaintiffs and the Nationwide Class**

347. Plaintiffs repeat and allege Paragraphs 1-295, as if fully alleged herein.

348. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

349. An actual controversy has arisen in the wake of the Marriott data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Marriott is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Personal Information. Plaintiffs allege that Marriott's data security measures remain inadequate. Marriott denies these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

350. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Marriott continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;
- b. Marriott continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

351. The Court also should issue corresponding prospective injunctive relief requiring Marriott to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

352. If an injunction is not issued, Plaintiffs and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Marriott. The risk of another such breach is real, immediate, and substantial. If another breach at Marriott occurs, Plaintiffs and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

353. The hardship to Plaintiffs and class members if an injunction does not issue exceeds the hardship to Marriott if an injunction is issued. Among other things, if another massive data breach occurs at Marriott, Plaintiff and class members will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Marriott of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Marriott has a pre-existing legal obligation to employ such measures.

354. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Marriott,

thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Personal Information would be further compromised.

**COUNT 7**

**MARYLAND PERSONAL INFORMATION PROTECTION ACT,**

*Md. Comm. Code §§ 14-3501, et seq.*

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Maryland Subclass

355. The Maryland Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Nationwide Class, or alternatively, on behalf of the Maryland Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

356. Under Md. Comm. Code § 14-3503(a), “[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations.”

357. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

358. Plaintiff and class members are “individuals” and “customers” as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

359. Plaintiff’s and class members’ Personal Information includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

360. Marriott did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

361. The Data Breach was a “breach of the security of a system” as defined by Md. Comm. Code § 14-3504(1).

362. Under Md. Comm. Code § 14-3504(b)(1), “[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach.”

363. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), “[i]f, after the investigation is concluded, the business determines that misuse of the individual’s Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach” and that notification “shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system.”

364. Because Marriott discovered a security breach and had notice of a security breach, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

365. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

366. As a direct and proximate result of Marriott’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and class members suffered damages, as described above.

367. Pursuant to Md. Comm. Code § 14-3508, Marriott’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of

the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101 et seq. and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

368. Plaintiff and class members seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

### **COUNT 8**

#### **MARYLAND CONSUMER PROTECTION ACT,**

*Md. Code Ann., Com. Law §§ 13-301, et seq.*

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Maryland Subclass

369. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nationwide Class, or alternatively, the Maryland Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

370. Marriott is a person as defined by Md. Code, Com Law § 13-101(h).

371. Marriott's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Code, Com. Law § 13-101(i) and § 13-303.

372. Nationwide Class members are "consumers" as defined by Md. Code, Com. Law § 13-101(c).

373. Marriott advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Code, Com. Law § 13-101(d).

374. Marriott advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

375. Marriott engaged in unfair and deceptive trade practices, in violation of Md. Code, Com. Law § 13-301, including:

- c. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;
- d. Representing that consumer goods or services have a characteristic that they do not have;
- e. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;
- f. Failing to state a material fact where the failure deceives or tends to deceive;
- g. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;
- h. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

376. Marriott engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services in violation of Md. Code, Com Law § 13-303, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and class members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

- previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and class members' Personal Information, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and class members' Personal Information; and
  - g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503.

377. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect

the confidentiality of consumers' Personal Information. Marriott's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

378. Marriott intended to mislead Plaintiff and class members and induce them to rely on its misrepresentations and omissions.

379. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the class members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

380. Marriott acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff and class members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

381. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations

alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

382. Plaintiff and class members seek all monetary and non-monetary relief allowed by law, including damages, restitution, disgorgement, injunctive relief, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE ALABAMA SUBCLASS**

**COUNT 9**

**ALABAMA DECEPTIVE TRADE PRACTICES ACT,**

*Ala. Code §§ 8-19-1, et seq.*

383. The Alabama Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alabama Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

384. Marriott is a "person" as defined by Ala. Code § 8-19-3(5).

385. Plaintiff and Alabama Subclass members are "consumers" as defined by Ala. Code § 8-19-3(2).

386. Plaintiff sent pre-suit notice pursuant to Ala. Code § 8-19-10(e) on January 8, 2019.

387. Marriott advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

388. Marriott engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and
- c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts.

389. Marriott's deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Alabama Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Alabama Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alabama Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

390. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

391. Marriott intended to mislead Plaintiff and Alabama Subclass members and induce them to rely on its misrepresentations and omissions.

392. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Alabama Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

393. Marriott acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Alabama Subclass

members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

394. As a direct and proximate result of Marriott's deceptive acts and practices, Plaintiff and Alabama Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

395. Marriott's deceptive acts and practices caused substantial injury to Plaintiff and Alabama Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

396. Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$100; treble damages; restitution; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE ALASKA SUBCLASS**

**COUNT 10**

**PERSONAL INFORMATION PROTECTION ACT,**

*Alaska Stat. §§ 45.48.010, et seq.*

397. The Alaska Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

398. Marriott is a business that owns or licenses Personal Information as defined by Alaska Stat. § 45.48.090(7). As such a business, it is a Covered Person as defined in Alaska Stat. § 45.48.010(a).

399. Plaintiff and Alaska Subclass members’ Personal Information includes Personal Information as covered under Alaska Stat. § 45.48.010(a).

400. Marriott is required to accurately notify Plaintiff and Alaska Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Alaska Stat. § 45.48.010(b).

401. Marriott is similarly required to determine the scope of the breach and restore the reasonable integrity of the information system under Alaska Stat. § 45.48.010(b).

402. Because Marriott was aware of a breach of its security system, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Alaska Stat. § 45.48.010(b).

403. By failing to disclose the Data Breach in a timely and accurate manner Marriott violated Alaska Stat. § 45.48.010(b).

404. Pursuant to Alaska Stat. § 45.48.080(b), a violation of Alaska Stat. § 45.48.010(b) is an unfair or deceptive act or practice under the Alaska Consumer Protection Act.

405. As a direct and proximate result of Marriott's violations of Alaska Stat. § 45.48.010(b), Plaintiff and Alaska Subclass members suffered damages, as described above.

406. Plaintiff and Alaska Subclass members seek relief measured as the greater of (a) each unlawful act, (b) three times actual damages in an amount to be determined at trial, or (c) statutory damages in the amount of \$500 for Plaintiff and each Alaska Subclass Member; reasonable attorneys' fees; and any other just and proper relief available under Alaska Stat. § 45.48.080(b)(2) and Alaska Stat. § 45.50.531.

### **COUNT 11**

#### **ALASKA CONSUMER PROTECTION ACT,**

*Alaska Stat. §§ 45.50.471, et seq.*

407. The Alaska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

408. Marriott advertised, offered, or sold goods or services in Alaska and engaged in trade or commerce directly or indirectly affecting the people of Alaska.

409. Alaska Subclass members are "consumers" as defined by Alaska Stat. § 45.50.561(4).

410. Marriott engaged in unfair or deceptive acts and practices in the conduct of trade or commerce, in violation Alaska Stat. § 45.50.471, including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade, when they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;

- d. Engaging in any other conduct creating a likelihood of confusion or of misunderstanding and which misleads, deceives, or damages a buyer in connection with the sale or advertisements of its goods or services; and
- e. Using or employing deception, fraud, false pretense, false promise, misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that others rely upon the concealment, suppression, or omission in connection with the sale or advertisement of its goods or services whether or not a person was in fact misled, deceived, or damaged.

411. Marriott's unfair and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Alaska Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Alaska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alaska Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

412. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

413. Marriott intended to mislead Plaintiff and Alaska Subclass members and induce them to rely on its misrepresentations and omissions.

414. Marriott acted intentionally, knowingly, and maliciously to violate Alaska's Consumer Protection Act, and recklessly disregarded Plaintiff and Alaska Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

415. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations

alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

416. Plaintiff and the Alaska Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) three times their actual damages or (b) statutory damages in the amount of \$500; punitive damages; reasonable attorneys' fees and costs; injunctive relief; and any other relief that is necessary and proper.

**CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS**

**COUNT 12**

**ARIZONA CONSUMER FRAUD ACT,**

*A.R.S. §§ 44-1521, et seq.*

417. The Arizona Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arizona Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

418. Marriott is a "person" as defined by A.R.S. § 44-1521(6).

419. Marriott advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

420. Marriott engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arizona Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arizona Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arizona Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

421. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

422. Marriott intended to mislead Plaintiff and Arizona Subclass members and induce them to rely on its misrepresentations and omissions.

423. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Arizona Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

424. Marriott acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff and Arizona Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

425. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations

alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

426. Plaintiff and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; restitution; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS**

**COUNT 13**

**ARKANSAS DECEPTIVE TRADE PRACTICES ACT,**

*A.C.A. §§ 4-88-101, et seq.*

427. The Arkansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

428. Marriott is a "person" as defined by A.C.A. § 4-88-102(5).

429. Marriott's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

430. Marriott advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

431. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, et seq., prohibits unfair, deceptive, false, and unconscionable trade practices.

432. Marriott engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or

omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

- a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services and as to goods being of a particular standard, quality, grade, style, or model;
- b. Advertising goods or services with the intent not to sell them as advertised;
- c. The employment of bait-and-switch advertising consistently of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell, as evidenced by acts demonstrating an intent not to sell the advertised product or services;
- d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of ignorance; and
- e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

433. Marriott's unconscionable, false, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arkansas Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arkansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b);
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arkansas Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b).

434. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

435. Marriott intended to mislead Plaintiff and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

436. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Plaintiff and the Arkansas Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

437. Marriott acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Arkansas Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

438. As a direct and proximate result of Marriott's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass members' reliance thereon, Plaintiff and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money

spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

439. Plaintiff and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; restitution; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS**

**COUNT 14**

**CALIFORNIA CUSTOMER RECORDS ACT,**

*Cal. Civ. Code §§ 1798.80, et seq.*

440. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

441. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

442. Marriott is a business that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass members.

443. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data

security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include “the types of Personal Information that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82.

444. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

445. Plaintiff and California Subclass members’ Personal Information includes Personal Information as covered by Cal. Civ. Code § 1798.82.

446. Because Marriott reasonably believed that Plaintiff’s and California Subclass members’ Personal Information was acquired by unauthorized persons during the Data Breach, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

447. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Cal. Civ. Code § 1798.82.

448. As a direct and proximate result of Marriott’s violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

449. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

**COUNT 15**

**CALIFORNIA UNFAIR COMPETITION LAW,**

*Cal. Bus. & Prof. Code §§ 17200, et seq.*

450. The California Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

451. Marriott is a “person” as defined by Cal. Bus. & Prof. Code §17201.

452. Marriott violated Cal. Bus. & Prof. Code §§ 17200, et seq. (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and practices.

453. Marriott’s “unfair” acts and practices include:

- a. Marriott failed to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members’ Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Marriott failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Personal Information has been compromised.

- b. Marriott's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.
- c. Marriott's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Marriott's inadequate security, consumers could not have reasonably avoided the harms that Marriott caused.
- d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

454. Marriott has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

455. Marriott's unlawful, unfair, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.

456. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

457. As a direct and proximate result of Marriott's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, the premiums and/or price received by Marriott for its goods and services, the loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

458. Marriott acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

459. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Marriott's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

**COUNT 16**

**CALIFORNIA CONSUMER LEGAL REMEDIES ACT,**

*Cal. Civ. Code §§ 1750, et seq.*

460. The California Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

461. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. (“CLRA”) is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

462. Marriott is a “person” as defined by Civil Code §§ 1761(c) and 1770, and has provided “services” as defined by Civil Code §§ 1761(b) and 1770.

463. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from “[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have.”

464. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from “[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another.”

465. Plaintiff and the California Class are “consumers” as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a “transaction” as defined by Civil Code §§ 1761(e) and 1770.

466. Marriott’s acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including, but not limited to, the following:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade when they were not;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

467. Marriott's representations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

468. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the California Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

469. As a direct and proximate result of Marriott's violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods

and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

470. Plaintiff and the California Subclass have provided notice of their claims for damages to Marriott, in compliance with California Civil Code § 1782(a).

471. Plaintiff and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

**CLAIMS ON BEHALF OF THE COLORADO SUBCLASS**

**COUNT 17**

**COLORADO SECURITY BREACH NOTIFICATION ACT,**

*Colo. Rev. Stat. §§ 6-1-716, et seq.*

472. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

473. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

474. Plaintiff and Colorado Subclass members' Personal Information includes Personal Information as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

475. Marriott is required to accurately notify Plaintiff and Colorado Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

476. Because Marriott was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

477. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Colo. Rev. Stat. § 6-1-716(2).

478. As a direct and proximate result of Marriott's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered damages, as described above.

479. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

### **COUNT 18**

#### **COLORADO CONSUMER PROTECTION ACT,**

*Colo. Rev. Stat. §§ 6-1-101, et seq.*

480. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

481. Marriott is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

482. Marriott engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

483. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Marriott or its successors in interest to actual consumers.

484. Marriott engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

- a. Knowingly making a false representation as to the characteristics of products and services;

- b. Representing that services are of a particular standard, quality, or grade, though Marriott knew or should have known that they were another;
- c. Advertising services with intent not to sell them as advertised; and
- d. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

485. Marriott's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Colorado Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Colorado Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Colorado Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

486. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

487. Marriott intended to mislead Plaintiff and Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

488. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Colorado Subclass members acted reasonably in

relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

489. Marriott acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

490. As a direct and proximate result of Marriott's deceptive trade practices, Colorado Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

491. Marriott's deceptive trade practices significantly impact the public because Marriott is the largest hotel chain in the world, with 30 brands with more than 7,000 properties in 131 countries and territories around the world.

492. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) \$500, or (c) three times actual damages (for Marriott's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE CONNECTICUT SUBCLASS**

**COUNT 19**

**CONNECTICUT UNFAIR TRADE PRACTICES ACT**

*C.G.S.A. § 42-110G*

**On Behalf of Plaintiffs and the Statewide Connecticut Subclass**

493. The Connecticut Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

494. As discussed herein, this count is subject to the Court's analysis under applicable choice of law principles.

495. Marriott is a "person" as defined by C.G.S.A. § 42-110a(3).

496. Marriott is engaged in "trade" or "commerce" as those terms are defined by C.G.S.A. § 42-110a(4).

497. At the time of filing this Complaint, Plaintiff has sent notice to the Attorney General and Commissioner of Consumer Protection pursuant to C.G.S.A. § 42-110g(c). Plaintiff will provide a file-stamped copy of the Complaint to the Attorney General and Commissioner of Consumer Protection.

498. Marriott advertised, offered, or sold services in Connecticut, and engaged in trade or commerce directly or indirectly affecting the people of Connecticut.

- a. Marriott engaged in deceptive acts and practices and unfair acts and practices in the conduct of trade or commerce, in violation of the C.G.S.A. § 42-110b, including:  
Representing that services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;
- b. Representing that services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and
- c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

499. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers.

500. Marriott intended to mislead Plaintiff and Connecticut Subclass members and induce them to rely on its misrepresentations and omissions.

501. Had Marriott disclosed to Plaintiff and Connecticut Subclass members that it misrepresented the security utilized on its networks, or otherwise had not omitted to Plaintiff and Connecticut Subclass members that its systems were insecure, Marriott would not have been able to continue storing Plaintiff and Connecticut Subclass members' Personal Information on its networks, and would have been forced to disclose the material information regarding security. Instead, Marriott and its predecessors allowed its servers to be hacked—undetected—over the course of four years, failed to discover that its servers were vulnerable through adequate due diligence and testing, and yet still continued to store customers' Personal Information in its databases.

502. Marriott's unlawful, deceptive, and unconscionable acts include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and class members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Connecticut Subclass members' Personal Information;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Connecticut Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Connecticut class members' Personal Information;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Connecticut Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Connecticut Subclass members' Personal Information.

503. Marriott's conduct is intentional, knowing, and malicious because Marriott knew the value of Personal Information it stored and failed to undertake or implement necessary safeguards, controls, and data security measures to keep it secure.

504. As a direct and proximate result of Marriott's deceptive acts and practices, Plaintiff and Connecticut Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from identity theft, fraudulent charges, and time and money spent on preventative and corrective measures.

505. Marriott's deceptive acts and practices caused substantial, ascertainable injury to Plaintiff and Connecticut Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

506. Marriott's violations of Connecticut law were done with reckless indifference to the Plaintiff and the Connecticut Subclass or was with an intentional or wanton violation of those rights.

507. Plaintiff requests damages in the amount to be determined at trial, including statutory and common law damages, restitution; attorneys' fees, and punitive damage.

**CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS**

**COUNT 20**

**DELAWARE COMPUTER SECURITY BREACH ACT,**

*6 Del. Code Ann. §§ 12B-102, et seq.*

508. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

509. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by 6 Del. Code Ann. § 12B-102(a).

510. Plaintiff and Delaware Subclass members' Personal Information includes Personal Information as covered under 6 Del. Code Ann. § 12B-101(4).

511. Marriott is required to accurately notify Plaintiff and Delaware Subclass members if Marriott becomes aware of a breach of its data security system which is reasonably likely to result in the misuse of a Delaware resident's Personal Information, in the most expedient time possible and without unreasonable delay under 6 Del. Code Ann. § 12B-102(a).

512. Because Marriott was aware of a breach of its security system which is reasonably likely to result in misuse of Delaware residents' Personal Information, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by 6 Del. Code Ann. § 12B-102(a).

513. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated 6 Del. Code Ann. § 12B-102(a).

514. As a direct and proximate result of Marriott's violations of 6 Del. Code Ann. § 12B-102(a), Plaintiff and Delaware Subclass members suffered damages, as described above.

515. Plaintiff and Delaware Subclass members seek relief under 6 Del. Code Ann. § 12B-104, including actual damages and equitable relief.

**COUNT 21**

**DELAWARE CONSUMER FRAUD ACT,**

*6 Del. Code §§ 2513, et seq.*

516. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

517. Marriott is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

518. Marriott advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

519. Marriott used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Delaware Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

- previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Delaware Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Delaware Subclass members' Personal Information; and
  - g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100.

520. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

521. Marriott acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiff and Delaware Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

522. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Delaware Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

523. Marriott's unlawful trade practices were gross, oppressive, and aggravated, and Marriott breached the trust of Plaintiff and the Delaware Subclass members.

524. As a direct and proximate result of Marriott's unlawful acts and practices, Plaintiff and Delaware Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and

money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

525. Plaintiff and Delaware Subclass members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Marriott's unlawful conduct; restitution; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE DISTRICT OF COLUMBIA SUBCLASS**

**COUNT 22**

**DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT,**

*D.C. Code §§ 28-3851, et seq.*

526. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

527. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by D.C. Code § 28-3852(a).

528. Plaintiff and District of Columbia Subclass members' Personal Information includes Personal Information as covered under D.C. Code § 28-3851(3).

529. Marriott is required to accurately notify Plaintiff and District of Columbia Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

530. Because Marriott was aware of a breach of its security system, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

531. By failing to disclose the Data Breach in a timely and accurate manner Marriott violated D.C. Code § 28-3852(a).

532. As a direct and proximate result of Marriott's violations of D.C. Code § 28-3852(a), Plaintiff and District of Columbia Subclass members suffered damages, as described above.

533. Plaintiff and District of Columbia Subclass members seek relief under D.C. Code § 28-3853(a), including actual damages.

### **COUNT 23**

#### **DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT,**

*D.C. Code §§ 28-3904, et seq.*

534. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

535. Marriott is a "person" as defined by D.C. Code § 28-3901(a)(1).

536. Marriott is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

537. Plaintiff and District of Columbia Subclass members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

538. Marriott advertised, offered, or sold goods or services in the District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of the District of Columbia.

539. Marriott engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

a. Representing that goods or services have characteristics that they do not have;

- b. Representing that goods or services are of a particular standard, quality, grade, style, or model, when they are of another;
- c. Misrepresenting a material fact that has a tendency to mislead;
- d. Failing to state a material fact where the failure is misleading;
- e. Advertising or offering goods or services without the intent to sell them as advertised or offered;
- f. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

540. Marriott's unfair, unlawful, and deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and District of Columbia Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and District of Columbia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and District of Columbia Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

541. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

542. Marriott intended to mislead Plaintiff and District of Columbia Subclass members and induce them to rely on its misrepresentations and omissions.

543. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and District of Columbia Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

544. Marriott acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiff and District of Columbia Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

545. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiff and District of Columbia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

546. Plaintiff and District of Columbia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or \$1500 per violation, and any other relief that the Court deems proper.

**CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS**

**COUNT 24**

**FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,**

*Fla. Stat. §§ 501.201, et seq.*

547. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

548. Plaintiff and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

549. Marriott advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

550. Marriott engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Florida Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Florida Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Florida Subclass members' Personal Information; and

- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

551. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

552. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Florida Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

553. As a direct and proximate result of Marriott's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for

fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

554. Plaintiff and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys’ fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS**

**COUNT 25**

**GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT,**

*Ga. Code Ann. §§ 10-1-370, et seq.*

555. The Georgia Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

556. Marriott, Plaintiff, and Georgia Subclass members are “persons” within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act (“Georgia UDTPA”).

557. Marriott engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code § 110-1-372(a), including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

558. Marriott’s deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Georgia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Georgia Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

559. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

560. Marriott intended to mislead Plaintiff and Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

561. In the course of its business, Marriott engaged in activities with a tendency or capacity to deceive.

562. Marriott acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

563. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Georgia Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

564. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the

benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

565. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under Ga. Code § 10-1-373.

**COUNT 26**

**RECOVERY OF EXPENSES OF LITIGATION ON BEHALF OF GEORGIA  
SUBCLASS**

*O.C.G.A. § 13-6-11*

566. The Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

567. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense."

568. Marriott through its actions alleged and described herein acted in bad faith, were stubbornly litigious, or caused the Georgia Subclass unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

569. The Georgia Subclass therefore requests that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

**CLAIMS ON BEHALF OF THE HAWAII SUBCLASS**

**COUNT 27**

**HAWAII SECURITY BREACH NOTIFICATION ACT,**

*Haw. Rev. Stat. §§ 487N-1, et seq.*

570. The Hawaii Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

571. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Haw. Rev. Stat. § 487N-2(a).

572. Plaintiff and Hawaii Subclass members’ Personal Information includes Personal Information as covered under Haw. Rev. Stat. § 487N-2(a).

573. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Haw. Rev. Stat. § 487N-2(a).

574. Plaintiff and Hawaii Subclass members’ Personal Information includes Personal Information as covered under Haw. Rev. Stat. § 487N-2(a).

575. Marriott is required to accurately notify Plaintiff and Hawaii Subclass members if it becomes aware of a breach of its data security system without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

576. Because Marriott was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

577. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Haw. Rev. Stat. § 487N-2(a).

578. As a direct and proximate result of Marriott's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass members suffered damages, as described above.

579. Plaintiff and Hawaii Subclass members seek relief under Haw. Rev. Stat. § 487N-3(b), including actual damages.

### **COUNT 28**

#### **HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT,**

*Haw. Rev. Stat. §§ 480-1, et seq.*

580. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

581. Plaintiff and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

582. Plaintiffs, the Hawaii Subclass members, and Marriott are "persons" as defined by Haw. Rev. Stat. § 480-1.

583. Marriott advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

584. Marriott engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

585. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

586. Marriott intended to mislead Plaintiff and Hawaii Subclass members and induce them to rely on its misrepresentations and omissions.

587. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

588. Marriott acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

589. As a direct and proximate result of Marriott's deceptive acts and practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

590. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

**COUNT 29**

**HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT,**

*Haw. Rev. Stat. §§ 481A-3, et seq.*

591. The Hawaii Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

592. Plaintiff and Hawaii Subclass members are “persons” as defined by Haw. Rev. Stat. § 481A-2.

593. Marriott engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

594. Marriott’s unfair and deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

595. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

596. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

597. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

598. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper.

**CLAIMS ON BEHALF OF THE IDAHO SUBCLASS**

**COUNT 30**

**IDAHO CONSUMER PROTECTION ACT,**

*Idaho Code §§ 48-601, et seq.*

599. The Idaho Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Idaho Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

600. Marriott is a "person" as defined by Idaho Code § 48-602(1).

601. Marriott's conduct as alleged herein pertained to "goods" and "services" as defined by Idaho Code § 48-602(6) and (7).

602. Marriott advertised, offered, or sold goods or services in Idaho and engaged in trade or commerce directly or indirectly affecting the people of Idaho.

603. Marriott engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- b. Representing that goods are of a particular standard, quality, or grade when they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in other acts and practices that are otherwise misleading, false, or deceptive to consumers;
- e. Engaging in unconscionable methods, acts or practices in the conduct of trade or commerce.

604. Marriott's unfair, deceptive, and unconscionable acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Idaho Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Idaho Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Idaho Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

605. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

606. Marriott intended to mislead Plaintiff and Idaho Subclass members and induce them to rely on its misrepresentations and omissions. Marriott knew its representations and omissions were false.

607. Marriott acted intentionally, knowingly, and maliciously to violate Idaho's Consumer Protection Act, and recklessly disregarded Plaintiff and Idaho Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

608. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable conduct, Plaintiff and Idaho Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

609. Plaintiff and Idaho Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, costs, and attorneys' fees.

**CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS**

**COUNT 31**

**ILLINOIS PERSONAL INFORMATION PROTECTION ACT,**

*815 Ill. Comp. Stat. §§ 530/10(a), et seq.*

610. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

611. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information, Marriott is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

612. Plaintiff and Illinois Subclass members' Personal Information includes Personal Information as covered under 815 Ill. Comp. Stat. § 530/5.

613. As a Data Collector, Marriott is required to notify Plaintiff and Illinois Subclass members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

614. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Marriott violated 815 Ill. Comp. Stat. § 530/10(a).

615. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

616. As a direct and proximate result of Marriott's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Illinois Subclass members suffered damages, as described above.

617. Plaintiff and Illinois Subclass members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Marriott's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

### **COUNT 32**

#### **ILLINOIS CONSUMER FRAUD ACT,**

*815 Ill. Comp. Stat. §§ 505, et seq.*

618. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

619. Marriott is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

620. Plaintiff and Illinois Subclass members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

621. Marriott's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

622. Marriott's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

623. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

624. Marriott intended to mislead Plaintiff and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

625. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

626. Marriott acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

627. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's

violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

628. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

### **COUNT 33**

#### **ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT,**

*815 Ill. Comp. Stat. §§ 510/2, et seq.*

629. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

630. Marriott is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

631. Marriott engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

632. Marriott's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and

Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

633. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

634. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

635. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

636. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

**CLAIMS ON BEHALF OF THE INDIANA SUBCLASS**

**COUNT 34**

**INDIANA DECEPTIVE CONSUMER SALES ACT,**

*Ind. Code §§ 24-5-0.5-1, et seq.*

637. The Indiana Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

638. Marriott is a “person” as defined by Ind. Code § 24-5-0.5-2(a)(2).

639. Marriott is a “supplier” as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits “consumer transactions,” within the meaning of § 24-5-0.5-2(a)(3)(A).

640. Marriott engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

641. Marriott’s representations and omissions include both implicit and explicit representations.

642. Marriott’s unfair, abusive, and deceptive acts, omissions, and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Indiana Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members’ Personal Information, including

- duties imposed by the FTC Act, 15 U.S.C. § 45, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Indiana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c);
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Indiana Subclass members' Personal Information; and
  - g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c).

643. Marriott's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

644. The injury to consumers from Marriott's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

645. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

646. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

647. Marriott's acts and practices were "abusive" for numerous reasons, including:

- a. because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Marriott's failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.
- b. because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Marriott's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.
- c. because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Marriott concerning the state of Marriott's security.
- d. because Marriott took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed four paragraphs below.

648. Marriott also engaged in “deceptive” acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

- a. Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;
- b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not;
- c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

649. Marriott intended to mislead Plaintiff and Indiana Subclass members and induce them to rely on its misrepresentations and omissions.

650. Marriott’s representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott’s data security and ability to protect the confidentiality of consumers’ Personal Information.

651. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs’ and class members’ Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott’s data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs’ and class members’ Personal

Information. Accordingly, Plaintiff and the Indiana Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

652. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because members of the public, including Plaintiff and the Indiana Subclass, repose a trust and confidence in Marriott to keep their Personal Information secure. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Indiana Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

653. Marriott acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate. Marriott's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

654. Plaintiff sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 on January 8, 2019. Marriott has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

655. Since Plaintiff provided the requisite notice, Marriott has failed to cure its violations of the Indiana Deceptive Consumer Sales Act.

656. Marriott's conduct includes incurable deceptive acts that Marriott engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

657. As a direct and proximate result of Marriott's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

658. Marriott's violations present a continuing risk to Plaintiff and Indiana Subclass members as well as to the general public.

659. Plaintiff and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$500 for each non-willful violation; the greater of treble damages or \$1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

**CLAIMS ON BEHALF OF THE IOWA SUBCLASS**

**COUNT 35**

**PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW,**

*Iowa Code § 715C.2*

660. The Iowa Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

661. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Iowa Code § 715C.2(1).

662. Plaintiff’s and Iowa Subclass members’ Personal Information includes Personal Information as covered under Iowa Code § 715C.2(1).

663. Marriott is required to accurately notify Plaintiff and Iowa Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

664. Because Marriott was aware of a breach of its security system, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1).

665. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Iowa Code § 715C.2(1).

666. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

667. As a direct and proximate result of Marriott’s violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass members suffered damages, as described above.

668. Plaintiff and Iowa Subclass members seek relief under Iowa Code § 714.16(7), including actual damages and injunctive relief.

**COUNT 36**

**IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT,**

*Iowa Code § 714H*

669. The Iowa Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

670. Marriott is a “person” as defined by Iowa Code § 714H.2(7).

671. Plaintiff and Iowa Subclass members are “consumers” as defined by Iowa Code § 714H.2(3).

672. Marriott’s conduct described herein related to the “sale” or “advertisement” of “merchandise” as defined by Iowa Code §§ 714H.2(2), (6), & (8).

673. Marriott engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Iowa Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members’ Personal Information, including

duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Iowa Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Iowa Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

674. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

675. Marriott intended to mislead Plaintiff and Iowa Subclass members and induce them to rely on its misrepresentations and omissions.

676. Marriott acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff and Iowa Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

677. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable conduct, Plaintiff and Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

678. Plaintiff has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

679. Plaintiff and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, punitive damages, and reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE KANSAS SUBCLASS**

#### **COUNT 37**

#### **PROTECTION OF CONSUMER INFORMATION**

*Kan. Stat. Ann. §§ 50-7a02(a), et seq.*

680. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

681. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

682. Plaintiff's and Kansas Subclass members' Personal Information includes Personal Information as covered under Kan. Stat. Ann. § 50-7a02(a).

683. Marriott is required to accurately notify Plaintiffs and Kansas Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

684. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass members' Personal Information, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

685. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Kan. Stat. Ann. § 50-7a02(a).

686. As a direct and proximate result of Marriott's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages, as described above.

687. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

### **COUNT 38**

#### **KANSAS CONSUMER PROTECTION ACT,**

*K.S.A. §§ 50-623, et seq.*

688. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

689. K.S.A. §§ 50-623, et seq. is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

690. Plaintiff and Kansas Subclass members are “consumers” as defined by K.S.A. § 50-624(b).

691. The acts and practices described herein are “consumer transactions,” as defined by K.S.A. § 50-624(c).

692. Marriott is a “supplier” as defined by K.S.A. § 50-624(l).

693. Marriott advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

694. Marriott engaged in deceptive and unfair acts or practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kansas Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas’s identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kansas Subclass members’ Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kansas Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

695. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

696. Marriott intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

697. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal

Information. Accordingly, Plaintiff and the Kansas Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

698. Marriott also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

- a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and
- b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Marriott knew were substantially one-sided in favor of Marriott (see K.S.A. § 50-627(b)(5)).

699. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Personal Information in Marriott's possession.

700. The above unfair, deceptive, and unconscionable practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

701. Marriott acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

702. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer

injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

703. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; restitution; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS**

**COUNT 39**

**KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT,**

*Ky. Rev. Stat. Ann. §§ 365.732, et seq.*

704. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

705. Marriott is required to accurately notify Plaintiff and Kentucky Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

706. Marriott is a business that holds computerized data that includes Personal Information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

707. Plaintiff's and Kentucky Subclass members' Personal Information includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

708. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

709. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Ky. Rev. Stat. Ann. § 365.732(2).

710. As a direct and proximate result of Marriott's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass members suffered damages, as described above.

711. Plaintiff and Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

#### **COUNT 40**

#### **KENTUCKY CONSUMER PROTECTION ACT,**

*Ky. Rev. Stat. §§ 367.110, et seq.*

712. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

713. Marriott is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

714. Marriott advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

715. Marriott engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kentucky Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kentucky Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kentucky Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and

Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

716. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

717. Marriott intended to mislead Plaintiff and Kentucky Subclass members and induce them to rely on its misrepresentations and omissions.

718. Plaintiff and Kentucky Subclass members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Marriott's unlawful acts and practices.

719. The above unlawful acts and practices by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

720. Marriott acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

721. As a direct and proximate result of Marriott's unlawful acts and practices, Plaintiff and Kentucky Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein;

losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

722. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS**

**COUNT 41**

**DATABASE SECURITY BREACH NOTIFICATION LAW,**

*La. Rev. Stat. Ann. §§ 51:3074(A), et seq.*

723. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

724. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

725. Plaintiff's and Louisiana Subclass members' Personal Information includes Personal Information as covered under La. Rev. Stat. Ann. § 51:3074(C).

726. Marriott is required to accurately notify Plaintiff and Louisiana Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

727. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

728. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated La. Rev. Stat. Ann. § 51:3074(C).

729. As a direct and proximate result of Marriott's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages, as described above.

730. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

#### **COUNT 42**

#### **LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW.**

*La Rev. Stat. Ann. §§ 51:1401, et seq.*

731. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

732. Marriott, Plaintiff, and the Louisiana Subclass members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

733. Plaintiff and Louisiana Subclass members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

734. Marriott engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

735. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or

commerce.” La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

736. Marriott participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Louisiana Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Louisiana Subclass members’ Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Louisiana Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

737. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

738. Marriott intended to mislead Plaintiff and Louisiana Subclass members and induce them to rely on its misrepresentations and omissions.

739. Marriott's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

740. Marriott acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

741. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the

law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Louisiana Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

742. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

743. Plaintiff and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Marriott's knowing violations of the Louisiana CPL; restitution; declaratory relief; attorneys' fees; and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE MAINE SUBCLASS**

**COUNT 43**

**MAINE UNFAIR TRADE PRACTICES ACT,**

*5 Me. Rev. Stat. §§ 205, 213, et seq.*

744. The Maine Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

745. Marriott is a “person” as defined by 5 Me. Rev. Stat. § 206(2).

746. Marriott’s conduct as alleged herein related was in the course of “trade and commerce” as defined by 5 Me. Rev. Stat. § 206(3).

747. Plaintiff and Maine Subclass members purchased goods and/or services for personal, family, and/or household purposes.

748. Plaintiff sent a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. § 213(1-A) on January 8, 2019.

749. Marriott engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

750. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

751. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal

Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Maine Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

752. As a direct and proximate result of Marriott's unfair and deceptive acts and conduct, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

753. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

#### **COUNT 44**

#### **MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT,**

*10 Me. Rev. Stat. §§ 1212, et seq.*

754. The Maine Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

755. Marriott is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

756. Marriott advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

757. Marriott engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. §1212, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

758. Marriott's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

759. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

760. Marriott intended to mislead Plaintiff and Maine Subclass members and induce them to rely on its misrepresentations and omissions.

761. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were

insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Maine Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

762. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

763. Maine Subclass members are likely to be damaged by Marriott's ongoing deceptive trade practices.

764. Plaintiff and the Maine Subclass members seek all relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS**

**COUNT 45**

**MASSACHUSETTS CONSUMER PROTECTION ACT,**

*Mass. Gen. Laws Ann. Ch. 93A, §§ 1, et seq.*

765. The Massachusetts Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

766. Marriott and Massachusetts Subclass members are “persons” as meant by Mass. Gen. Laws. Ann. ch. 93A, § 1(a).

767. Marriott operates in “trade or commerce” as meant by Mass. Gen. Laws Ann. ch. 93A, § 1(b).

768. Marriott advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. ch. 93A, § 1(b).

769. Plaintiff sent a demand for relief on behalf of the Massachusetts Subclass pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3) on January 8, 2019.

770. Marriott engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. ch. 93A, § 2(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Massachusetts Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, §

- 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Massachusetts Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Massachusetts Subclass members' Personal Information; and
  - g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

771. Marriott's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Marriott solely held the true facts about its inadequate security for Personal Information, which Plaintiff and the Massachusetts Subclass members could not independently discovered.

772. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

773. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

774. Marriott intended to mislead Plaintiff and Massachusetts Subclass members and induce them to rely on its misrepresentations and omissions. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

775. Marriott acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff and Massachusetts Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

776. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and Massachusetts Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for

fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

777. Plaintiff and Massachusetts Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, restitution; injunctive or other equitable relief, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS**

**COUNT 46**

**MICHIGAN IDENTITY THEFT PROTECTION ACT,**

*Mich. Comp. Laws Ann. §§ 445.72, et seq.*

778. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

779. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

780. Plaintiff's and Michigan Subclass members' Personal Information includes Personal Information as covered under Mich. Comp. Laws Ann. § 445.72(1).

781. Marriott is required to accurately notify Plaintiff and Michigan Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

782. Because Marriott discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

783. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Mich. Comp. Laws Ann. § 445.72(4).

784. As a direct and proximate result of Marriott's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass members suffered damages, as described above.

785. Plaintiff and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

#### **COUNT 47**

#### **MICHIGAN CONSUMER PROTECTION ACT,**

*Mich. Comp. Laws Ann. §§ 445.903, et seq.*

786. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

787. Marriott and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

788. Marriott advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

789. Marriott engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);
- b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

- c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and
- d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

790. Marriott's unfair, unconscionable, and deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Michigan Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Michigan Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Michigan Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

791. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

792. Marriott intended to mislead Plaintiff and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

793. Marriott acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

794. As a direct and proximate result of Marriott's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott

for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

795. Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$250, restitution, injunctive relief, and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS**

**COUNT 48**

**MINNESOTA CONSUMER FRAUD ACT,**

*Minn. Stat. §§ 325F.68, et seq. and Minn. Stat. §§ 8.31, et seq.*

796. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

797. Marriott, Plaintiff, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

798. Marriott's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

799. Marriott engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

800. Marriott engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Minnesota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and

Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

801. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

802. Marriott intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

803. Marriott's fraudulent, misleading, and deceptive practices affected the public interest, including the Minnesotans affected by the Data Breach.

804. As a direct and proximate result of Marriott's fraudulent, misleading, and deceptive practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

805. Plaintiff and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

**COUNT 49**

**MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT,**

*Minn. Stat. §§ 325D.43, et seq.*

806. The Minnesota Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

807. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Marriott violated Minn. Stat. § 325D.44, including the following provisions:

- a. Representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);
- b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);
- c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and
- d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

808. Marriott’s deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

- previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Minnesota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Personal Information; and
  - g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

809. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

810. Marriott intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

811. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Minnesota Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

812. Marriott acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Minnesota Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

813. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and

money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

814. Plaintiff and Minnesota Subclass members seek, including injunctive relief and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE MISSISSIPPI SUBCLASS**

**COUNT 50**

**MISSISSIPPI CONSUMER PROTECTION ACT,**

*Miss. Code §§ 75-24-1, et seq.*

815. The Mississippi Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Mississippi Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

816. Marriott is a "person," as defined by Miss. Code § 75-24-3.

817. Marriott advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3.

818. Plaintiff has complied with all pre-conditions for bringing a private action under Miss. Code § 75-24-15.

819. Marriott engaged in unfair and deceptive trade acts or practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Mississippi Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Mississippi Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Mississippi Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

820. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised.

821. Marriott intended to mislead Plaintiff and Mississippi Subclass members and induce them to rely on its misrepresentations and omissions.

822. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

823. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Mississippi Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

824. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Mississippi Subclass—and Marriott, because consumers are unable to

fully protect their interests with regard to their data, and placed trust and confidence in Marriott.

Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Mississippi Subclass that contradicted these representations.

825. Marriott acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiff and Mississippi Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

826. As a direct and proximate result of Marriott's unfair and deceptive acts or practices and Plaintiff and Mississippi Subclass members' purchase of goods or services primarily for personal, family, or household purposes, Plaintiff and Mississippi Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

827. Marriott's violations present a continuing risk to Plaintiff and Mississippi Subclass members as well as to the general public.

828. Plaintiff and Mississippi Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS**

**COUNT 51**

**MISSOURI MERCHANDISING PRACTICES ACT,**

*Mo. Rev. Stat. §§ 407.010, et seq.*

829. The Missouri Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

830. Marriott is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

831. Marriott advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

832. Plaintiff and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

833. Marriott engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Missouri Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

- previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Missouri Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Missouri Subclass members' Personal Information; and
  - g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

834. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

835. Marriott intended to mislead Plaintiff and Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

836. Marriott acted intentionally, knowingly, and maliciously to violate Missouri's Merchandising Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

837. As a direct and proximate result of Marriott's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

838. Plaintiff and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

**CLAIMS ON BEHALF OF THE MONTANA SUBCLASS**

**COUNT 52**

**COMPUTER SECURITY BREACH LAW,**

*Mont. Code Ann. §§ 30-14-1704(1), et seq.*

839. The Montana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

840. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Mont. Code Ann. § 30-14-1704(4)(b). Marriott also maintains computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to Mont. Code Ann. § 30-14-1704(1) and (2).

841. Plaintiff's and Montana Subclass members' Personal Information includes Personal Information covered by Mont. Code Ann. § 30-14-1704(4)(b).

842. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Plaintiff and Montana Subclass members, pursuant to Mont. Code Ann. § 30-14-1704(2).

843. Marriott is required to accurately notify Plaintiff and Montana Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Marriott owns or licenses, without unreasonable delay under Mont. Code Ann. § 30-14-1704(1).

844. Because Marriott was aware of a security breach, Marriott had an obligation to disclose the data breach as mandated by Mont. Code Ann. § 30-14-1704(1) and (2).

845. Pursuant to Mont. Code Ann. § 30-14-1705, violations of Mont. Code Ann. § 30-14-1704 are unlawful practices under Mont. Code Ann. § 30-14-103, Montana's Consumer Protection Act.

846. As a direct and proximate result of Marriott's violations of Mont. Code Ann. § 30-14-1704(1) and (2), Plaintiff and Montana Subclass members suffered damages, as described above.

847. Plaintiff and Montana Subclass members seek relief under Mont. Code Ann. § 30-14-133, including actual damages and injunctive relief.

**COUNT 53**

**MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT,**

*M.C.A. §§ 30-14-101, et seq.*

848. The Montana Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

849. Marriott is a “person” as defined by MCA § 30-14-102(6).

850. Plaintiff and Montana Subclass members are “consumers” as defined by MCA § 30-14-102(1).

851. Marriott advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by MCA § 30-14-102(8).

852. Marriott engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation MCA § 30-14-103, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Montana Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members’ Personal Information, including

duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Montana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Montana Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

853. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

854. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were

insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Montana Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

855. Marriott's acts described above are unfair and offend public policy; they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

856. Marriott acted intentionally, knowingly, and maliciously to violate Montana's Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiff and Montana Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

857. As a direct and proximate result of Marriott's unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiff and Montana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

858. Plaintiff and Montana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$500,

treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

**CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS**

**COUNT 54**

**NEBRASKA CONSUMER PROTECTION ACT,**

*Neb. Rev. Stat. §§ 59-1601, et seq.*

859. The Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

860. Marriott and Nebraska Subclass members are each a "person" as defined by Neb. Rev. Stat. § 59-1601(1).

861. Marriott advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

862. Marriott engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nebraska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

863. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

864. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

865. Marriott's unfair and deceptive acts and practices complained of herein affected the public interest, including the many Nebraskans affected by the Data Breach.

866. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either actual damages or \$1,000, civil penalties, and reasonable attorneys' fees and costs.

### **COUNT 55**

#### **NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT,**

*Neb. Rev. Stat. §§ 87-301, et seq.*

867. The Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

868. Marriott and Nebraska Subclass members are "persons" as defined by Neb. Rev. Stat. § 87-301(19).

869. Marriott advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

870. Marriott engaged in deceptive trade practices in the course of its business, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including:

- a. Represented that goods and services have characteristics, uses, benefits, or qualities that they do not have;
- b. Represented that goods and services are of a particular standard, quality, or grade if they are of another; and
- c. Advertised its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

871. Marriott's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nebraska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

872. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

873. Marriott intended to mislead Plaintiff and Nebraska Subclass members and induce them to rely on its misrepresentations and omissions.

874. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Nebraska Subclass members acted reasonably in

relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

875. Marriott acted intentionally, knowingly, and maliciously to violate Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nebraska Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

876. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

877. Marriott's deceptive trade practices complained of herein affected consumers at large, including the large percentage of Nebraskans affected by the Data Breach.

878. Plaintiff and Nebraska Subclass members seek all relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE NEVADA SUBCLASS**

**COUNT 56**

**NEVADA DECEPTIVE TRADE PRACTICES ACT,**

*Nev. Rev. Stat. Ann. §§ 598.0903 et seq.*

879. The Nevada Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

880. Marriott advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

881. Marriott engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including:

- a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5);
- b. Representing that goods or services for sale are of a particular standard, quality, or grade when Marriott knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);
- c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat § 598.0915(9);
- d. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(2); and
- e. Violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

882. Marriott’s deceptive trade practices in the course of its business or occupation include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nevada Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nevada Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nevada Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and

Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210.

883. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

884. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Nevada Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

885. Marriott acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

886. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Nevada Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein;

losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

887. Plaintiff and Nevada Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS**

**COUNT 57**

**NOTICE OF SECURITY BREACH**

*N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), et seq.*

888. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

889. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

890. Plaintiff's and New Hampshire Subclass members' Personal Information includes Personal Information as covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

891. Marriott is required to accurately notify Plaintiff and New Hampshire Subclass members if Marriott becomes aware of a breach of its data security system in which misuse of Personal Information has occurred or is reasonably likely to occur, as soon as possible under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

892. Because Marriott was aware of a security breach in which misuse of Personal Information has occurred or is reasonably likely to occur, Marriott had an obligation to disclose

the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

893. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

894. As a direct and proximate result of Marriott's violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass members suffered damages, as described above.

895. Plaintiff and New Hampshire Subclass members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including actual damages and injunctive relief.

### **COUNT 58**

#### **NEW HAMPSHIRE CONSUMER PROTECTION ACT,**

*N.H.R.S.A. §§ 358-A, et seq.*

896. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

897. Marriott is a "person" under the New Hampshire Consumer Protection.

898. Marriott advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H.R.S.A. § 358-A:1.

899. Marriott engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H.R.S.A. § 358-A:2, including:

- a. Representing that its goods or services have characteristics, uses, or benefits that they do not have in violation of N.H.R.S.A. § 358-A:2.V;

- b. Representing that its goods or services are of a particular standard or quality if they are of another in violation of N.H.R.S.A. § 358-A:2.VII; and
- c. Advertising its goods or services with intent not to sell them as advertised in violation of N.H.R.S.A. § 358-A:2.IX.

900. Marriott's unfair and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Hampshire Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Hampshire Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Hampshire Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

901. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

902. Marriott acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiff and New Hampshire Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate. Marriott's acts and practices went beyond the realm of strictly private transactions.

903. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent

activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

904. Plaintiff and New Hampshire Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS**

**COUNT 59**

**NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT,**

*N.J. Stat. Ann. §§ 56:8-163, et seq.*

905. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

906. Marriott is a business that conducts business in New Jersey under N.J. Stat. Ann. § 56:8-163(a).

907. Plaintiff's and New Jersey Subclass members' Personal Information includes Personal Information covered under N.J. Stat. Ann. §§ 56:8-163, et seq.

908. Under N.J. Stat. Ann. § 56:8-163(a), "[a]ny business that conducts business in New Jersey. . . shall disclose any breach of security of [] computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

909. Because Marriott discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, et seq.

910. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated N.J. Stat. Ann. § 56:8-163(a).

911. As a direct and proximate result of Marriott's violations of N.J. Stat. Ann. § 56:8-163(a), Plaintiff and New Jersey Subclass members suffered the damages described above.

912. Plaintiff and New Jersey Subclass members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

### **COUNT 60**

#### **NEW JERSEY CONSUMER FRAUD ACT,**

*N.J. Stat. Ann. §§ 56:8-1, et seq.*

913. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

914. Marriott is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

915. Marriott sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

916. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

917. Marriott's unconscionable and deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Jersey Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Jersey Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

918. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

919. Marriott intended to mislead Plaintiff and New Jersey Subclass members and induce them to rely on its misrepresentations and omissions.

920. Marriott acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff and New Jersey Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

921. As a direct and proximate result of Marriott's unconscionable and deceptive practices, Plaintiff and New Jersey Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

922. Plaintiff and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

**CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS**

**COUNT 61**

**NEW MEXICO UNFAIR PRACTICES ACT,**

*N.M. Stat. Ann. §§ 57-12-2, et seq.*

923. The New Mexico Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

924. Marriott is a “person” as meant by N.M. Stat. Ann. § 57-12-2.

925. Marriott was engaged in “trade” and “commerce” as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

926. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, et seq., prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

927. Marriott engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following:

- a. Knowingly representing that its goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. § 57-12-2(D)(5);
- b. Knowingly representing that its goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. § 57-12-2(D)(7);
- c. Knowingly using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive in violation of N.M. Stat. Ann. § 57-12-2(D)(14)

- d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff's and the New Mexico Subclass' detriment in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and
- e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).

928. Marriott's unfair, deceptive, and unconscionable acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Mexico Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Mexico Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes mandating reasonable data security, N.M. Stat. § 57-12C-4;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Mexico Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes mandating reasonable data security, N.M. Stat. § 57-12C-4.

929. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

930. Marriott intended to mislead Plaintiff and New Mexico Subclass members and induce them to rely on its misrepresentations and omissions.

931. Marriott acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

932. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Subclass members have suffered and will continue to

suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

933. Plaintiff and New Mexico Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of \$100 (whichever is greater), treble damages or statutory damages of \$300 (whichever is greater), and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS**

**COUNT 62**

**NEW YORK GENERAL BUSINESS LAW.**

*N.Y. Gen. Bus. Law §§ 349, et seq.*

934. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

935. Marriott engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New York Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New York Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

936. Plaintiff and members of the New York Subclass were deceived in New York. They also transacted with Marriott in New York by making hotel reservations from New York and/or staying in Marriott properties based in New York.

937. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

938. Marriott acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

939. As a direct and proximate result of Marriott's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

940. Marriott's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Data Breach.

941. The above deceptive and unlawful practices and acts by Marriott caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

942. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

**CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS**

**COUNT 63**

**NORTH CAROLINA IDENTITY THEFT PROTECTION ACT,**

*N.C. Gen. Stat. §§ 75-60, et seq.*

943. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

944. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

945. Plaintiff and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

946. Marriott is required to accurately notify Plaintiff and North Carolina Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

947. Plaintiff's and North Carolina Subclass members' Personal Information includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

948. Because Marriott discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by

unauthorized persons), Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

949. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated N.C. Gen. Stat. § 75-65.

950. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

951. As a direct and proximate result of Marriott's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass members suffered damages, as described above.

952. Plaintiff and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

#### **COUNT 64**

#### **NORTH CAROLINA UNFAIR TRADE PRACTICES ACT,**

*N.C. Gen. Stat. Ann. §§ 75-1.1, et seq.*

953. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

954. Marriott advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

955. Marriott engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Carolina Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and North Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Carolina Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

956. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

957. Marriott intended to mislead Plaintiff and North Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

958. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the North Carolina Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

959. Marriott acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

960. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods

and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

961. Marriott's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

962. Plaintiff and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, restitution, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE NORTH DAKOTA SUBCLASS**

**COUNT 65**

**NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION.**

*N.D. Cent. Code §§ 51-30-02, et seq.*

963. The North Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

964. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.D. Cent. Code § 51-30-01(4). Marriott also maintains computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to N.D. Cent. Code §§ 51-30-02 and 03.

965. Plaintiff's and North Dakota Subclass members' Personal Information includes Personal Information covered by N.D. Cent. Code § 51-30-01(4).

966. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Plaintiff and North Dakota Subclass members, pursuant to N.D. Cent. Code § 51-30-03.

967. Marriott is required to accurately notify Plaintiff and North Dakota Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Marriott owns or licenses, in the most expedient time possible and without unreasonable delay under N.D. Cent. Code § 51-30-02.

968. Because Marriott was aware of a security breach, Marriott had an obligation to disclose the data breach as mandated by N.D. Cent. Code §§ 51-30-02 and 51-30-03.

969. Pursuant to N.D. Cent. Code § 51-30-07, violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03 are unlawful sales or advertising practices which violate chapter 51-15 of the North Dakota Century Code.

970. As a direct and proximate result of Marriott's violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03, Plaintiff and North Dakota Subclass members suffered damages, as described above.

971. Plaintiff and North Dakota Subclass members seek relief under N.D. Cent. Code §§ 51-15-01 et seq., including actual damages and injunctive relief.

#### **COUNT 66**

#### **NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT,**

*N.D. Cent. Code §§ 51-15-01, et seq.*

972. The North Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

973. Marriott, Plaintiff, and each member of the North Dakota Subclass is a “person,” as defined by N.D. Cent. Code § 51-15-01(4).

974. Marriott sells and advertises “merchandise,” as defined by N.D. Cent. Code § 51-15-01(3) and (5).

975. Marriott advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

976. Marriott engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code § 51-15-01, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Dakota Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and North Dakota Subclass members’ Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Dakota Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

977. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

978. The Marriott's above-described acts and practices caused substantial injury to Plaintiff and North Dakota Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

979. Marriott intended to mislead Plaintiff and North Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

980. Marriott acted intentionally, knowingly, and maliciously to violate North Dakota's Unlawful Sales or Advertising Law, and recklessly disregarded Plaintiff and North Dakota Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

981. As a direct and proximate result of Marriott's deceptive, unconscionable, and substantially injurious practices, Plaintiff and North Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

982. Plaintiff and North Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

**CLAIMS ON BEHALF OF THE OHIO SUBCLASS**

**COUNT 67**

**OHIO CONSUMER SALES PRACTICES ACT,**

*Ohio Rev. Code §§ 1345.01, et seq.*

983. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

984. Plaintiff and Ohio Subclass members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

985. Marriott was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

986. Marriott advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

987. Marriott engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including:

- a. Marriott represented that its goods, services, and intangibles had performance characteristics, uses, and benefits that it did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and
- b. Marriott represented that its goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

988. Marriott engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including:

- a. Marriott knowingly took advantage of the inability of Plaintiff and the Ohio Subclass to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and
- b. Marriott required Plaintiff and the Ohio Subclass to enter into a consumer transaction on terms that Marriott knew were substantially one-sided in favor of Marriott (Ohio Rev. Code Ann. § 1345.03(B)(5)).

989. Marriott's unfair, deceptive, and unconscionable acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

990. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

991. Marriott intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

992. Marriott acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

993. Marriott's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the Data Breach.

994. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable acts and practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

995. Plaintiff and the Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

### **COUNT 68**

#### **OHIO DECEPTIVE TRADE PRACTICES ACT,**

*Ohio Rev. Code §§ 4165.01, et seq.*

996. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

997. Marriott, Plaintiff, and Ohio Subclass members are each a “person,” as defined by Ohio Rev. Code § 4165.01(D).

998. Marriott advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

999. Marriott engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

- a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);
- b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and
- c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

1000. Marriott’s deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1001. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1002. Marriott intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

1003. Marriott acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1004. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses

of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1005. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, restitution, attorneys' fees, and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS**

**COUNT 69**

**OKLAHOMA CONSUMER PROTECTION ACT,**

*Okla. Stat. Tit. 15, §§ 751, et seq.*

1006. The Oklahoma Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1007. Marriott is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

1008. Marriott's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

1009. Marriott, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

- a. Made false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5);
- b. Represented, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7);
- c. Advertised, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8);
- d. Committed unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and
- e. Committed deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

1010. Marriott's unlawful practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oklahoma Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oklahoma Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oklahoma Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1011. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1012. Marriott intended to mislead Plaintiff and Oklahoma Subclass members and induce them to rely on its misrepresentations and omissions.

1013. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business

and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Oklahoma Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1014. The above unlawful practices and acts by Marriott were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Oklahoma Subclass members.

1015. Marriott acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1016. As a direct and proximate result of Marriott's unlawful practices, Plaintiff and Oklahoma Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money

spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1017. Plaintiff and Oklahoma Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE OREGON SUBCLASS**

**COUNT 70**

**OREGON CONSUMER IDENTITY THEFT PROTECTION ACT,**

*Or. Rev. Stat. §§ 646A.604(1), et seq.*

1018. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1019. Marriott is a business that maintains records which contain Personal Information, within the meaning of Or. Rev. Stat. § 646A.622(1), about Plaintiff and Oregon Subclass members.

1020. Pursuant to Or. Rev. Stat. § 646A.622(1), a business "that maintains records which contain Personal Information" of an Oregon resident "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

1021. Marriott violated Or. Rev. Stat. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiff's and Oregon Subclass members' Personal Information.

1022. Marriott is a business that owns, maintains, or otherwise possesses data that includes consumers Personal Information as defined by Or. Rev. Stat. § 646A.604(1).

1023. Plaintiff's and Oregon Subclass members' Personal Information includes Personal Information as covered under Or. Rev. Stat. § 646A.604(1).

1024. Marriott is required to accurately notify Plaintiff and Oregon Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. § 646A.604(1).

1025. Because Marriott discovered a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. § 646A.604(1).

1026. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Or. Rev. Stat. § 646A.604(1).

1027. Pursuant to Or. Rev. Stat. § 646A.604(9), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

1028. As a direct and proximate result of Marriott's violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass members suffered damages, as described above.

1029. Plaintiff and Oregon Subclass members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

## **COUNT 71**

### **OREGON UNLAWFUL TRADE PRACTICES ACT,**

*Or. Rev. Stat. §§ 646.608, et seq.*

1030. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1031. Marriott is a "person," as defined by Or. Rev. Stat. § 646.605(4).

1032. Marriott engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

1033. Marriott sold “goods or services,” as defined by Or. Rev. Stat. § 646.605(6)(a).

1034. Marriott advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

1035. Marriott engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

- a. Represented that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);
- b. Represented that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);
- c. Advertised its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and
- d. Concurrent with tender or delivery of its goods and services, failed to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

1036. Marriott’s unlawful practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oregon Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members’ Personal Information, including

- duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq., which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oregon Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oregon
  - g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.

1037. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1038. Marriott intended to mislead Plaintiff and Oregon Subclass members and induce them to rely on its misrepresentations and omissions.

1039. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Oregon Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1040. Marriott acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1041. As a direct and proximate result of Marriott's unlawful practices, Plaintiff and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1042. Plaintiff and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, restitution, actual damages or statutory damages of \$200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS**

**COUNT 72**

**PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION  
LAW,**

*73 Pa. Cons. Stat. §§ 201-2 & 201-3, et seq.*

1043. The Pennsylvania Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1044. Marriott is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

1045. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

1046. Marriott Pennsylvania engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

- a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));
- b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and
- c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

1047. Marriott's unfair or deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Pennsylvania Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Pennsylvania Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Pennsylvania Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and

Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1048. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1049. Marriott intended to mislead Plaintiff and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

1050. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Pennsylvania Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1051. Marriott acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1052. As a direct and proximate result of Marriott's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass' reliance on

them, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1053. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

**CLAIMS ON BEHALF OF THE PUERTO RICO SUBCLASS**

**COUNT 73**

**CITIZEN INFORMATION ON DATA BANKS SECURITY ACT,**

*P.R. Laws Ann. tit. 10, §§ 4051, et seq.*

1054. Plaintiffs, on behalf of the Puerto Rico Subclass, repeat and allege Paragraphs 1-295, as if fully alleged herein.

1055. Marriott is the owner and custodian of databases that include Personal Information as defined by P.R. Laws Ann. Tit. 10, § 4051(a), and is therefore subject to. P.R. Laws Ann. Tit. 10, § 4052.

1056. Plaintiff's and Puerto Rico Subclass members' Personal Information includes personal identifying information as covered under P.R. Laws Ann. Tit. 10, § 4051(a).

1057. Marriott is required to accurately notify Plaintiff and Puerto Rico Subclass members following discovery or notification of a breach of its data security system as expeditiously as possible under P.R. Laws Ann. Tit. 10, § 4052.

1058. Because Marriott discovered a breach of its data security system, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by P.R. Laws Ann. Tit. 10, § 4052.

1059. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated P.R. Laws Ann. Tit. 10, § 4052.

1060. As a direct and proximate result of Marriott's violations of P.R. Laws Ann. Tit. 10, § 4052, Plaintiff and Puerto Rico Subclass members suffered damages, as described above.

1061. Plaintiff and Puerto Rico Subclass members seek relief under P.R. Laws Ann. Tit. 10, § 4055, including actual damages and injunctive relief.

### **CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS**

#### **COUNT 74**

#### **RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT,**

*R.I. Gen. Laws §§ 6-13.1, et seq.*

1062. The Rhode Island Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Rhode Island Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1063. Plaintiff and Rhode Island Subclass members are each a "person," as defined by R.I. Gen. Laws § 6-13.1-1(3).

1064. Plaintiff and Rhode Island Subclass members purchased goods and services for personal, family, or household purposes.

1065. Marriott advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

1066. Marriott engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-52(6)(v));
- b. Representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-52(6)(vii));
- c. Advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-52(6)(ix));
- d. Engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-52(6)(xii));
- e. Engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-52(6)(xiii)); and
- f. Using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-52(6)(xiv)).

1067. Marriott's unfair and deceptive acts include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Rhode Island Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

- previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Rhode Island Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Rhode Island Subclass members' Personal Information; and
  - g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2.

1068. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1069. Marriott intended to mislead Plaintiff and Rhode Island Subclass members and induce them to rely on its misrepresentations and omissions.

1070. Marriott acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Rhode Island Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1071. As a direct and proximate result of Marriott's unfair and deceptive acts, Plaintiff and Rhode Island Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1072. Plaintiff and Rhode Island Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$200 per Subclass Member (whichever is greater), punitive damages, injunctive relief, restitution and other equitable relief, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS**

**COUNT 75**

**SOUTH CAROLINA DATA BREACH SECURITY ACT,**

*S.C. Code Ann. §§ 39-1-90, et seq.*

1073. The South Carolina Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1074. Marriott is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

1075. Plaintiff’s and South Carolina Subclass members’ Personal Information includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

1076. Marriott is required to accurately notify Plaintiff and South Carolina Subclass members following discovery or notification of a breach of its data security system if Personal Information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

1077. Because Marriott discovered a breach of its data security system in which Personal Information that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

1078. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated S.C. Code Ann. § 39-1-90(A).

1079. As a direct and proximate result of Marriott's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and South Carolina Subclass members suffered damages, as described above.

1080. Plaintiff and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

### **COUNT 76**

#### **SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT,**

*S.C. Code Ann. §§ 39-5-10, et seq.*

1081. The South Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1082. Marriott is a "person," as defined by S.C. Code Ann. § 39-5-10(a).

1083. South Carolina's Unfair Trade Practices Act (SC UTPA) prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

1084. Marriott advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

1085. Marriott engaged in unfair and deceptive acts and practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and South Carolina Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and South Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and South Carolina Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1086. Marriott's acts and practices had, and continue to have, the tendency or capacity to deceive.

1087. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1088. Marriott intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1089. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the South Carolina Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1090. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiff and the South Carolina Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to the Personal Information in Marriott's possession, and place trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Carolina Subclass that contradicted these representations.

1091. Marriott's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Marriott's acts and practices offend established public policies that seek to protect consumers' Personal Information and ensure that entities entrusted with Personal Information use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45, and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, et seq.

1092. Marriott's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of Marriott's long history of inadequate data security and previous data breaches and the sensitivity and extensivity of Personal Information in its possession.

1093. Marriott's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Marriott engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including the many South Carolinians impacted by the Data Breach.

1094. Marriott's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Marriott's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

1095. Marriott's violations present a continuing risk to Plaintiff and South Carolina Subclass members as well as to the general public.

1096. Marriott intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1097. Marriott acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and South Carolina Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct, and would deter Marriott and others from committing similar conduct in the future.

1098. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiff and South Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1099. Plaintiff and South Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE SOUTH DAKOTA SUBCLASS**

**COUNT 77**

**SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT,**

*S.D. Codified Laws §§ 37-24-1, et seq.*

1100. The South Dakota Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the South Dakota Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1101. Marriott is a “person,” as defined by S.D. Codified Laws § 37-24-1(8).

1102. Marriott advertises and sells “merchandise,” as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1103. Marriott advertised, offered, or sold goods or services in South Dakota and engaged in trade or commerce directly or indirectly affecting the people of South Dakota, as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1104. Marriott knowingly engaged in deceptive acts or practices, misrepresentation, concealment, suppression, or omission of material facts in connection with the sale and advertisement of goods or services, in violation of S.D. Codified Laws § 37-24-6, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and South Dakota Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and South Dakota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and South Dakota Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1105. Marriott intended to mislead Plaintiff and South Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

1106. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1107. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the South Dakota Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1108. Marriott had a duty to disclose the above facts because Plaintiff and the South Dakota Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the South Dakota Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and have placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Dakota Subclass that contradicted these representations.

1109. As a direct and proximate result of Marriott's deceptive acts or practices, misrepresentations, and concealment, suppression, and/or omission of material facts, Plaintiff and South Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1110. Marriott's violations present a continuing risk to Plaintiff and South Dakota Subclass members as well as to the general public.

1111. Plaintiff and South Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS**

**COUNT 78**

**TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT,**

*Tenn. Code Ann. §§ 47-18-2107, et seq.*

1112. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1113. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

1114. Plaintiff's and Tennessee Subclass members' Personal Information includes Personal Information as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

1115. Marriott is required to accurately notify Plaintiff and Tennessee Subclass members following discovery or notification of a breach of its data security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

1116. Because Marriott discovered a breach of its security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

1117. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Tenn. Code Ann. § 47-18-2107(b).

1118. As a direct and proximate result of Marriott's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

1119. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

### **COUNT 79**

#### **TENNESSEE CONSUMER PROTECTION ACT,**

*Tenn. Code Ann. §§ 47-18-101, et seq.*

1120. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1121. Marriott is a “person,” as defined by Tenn. Code § 47-18-103(13).

1122. Plaintiff and Tennessee Subclass members are “consumers,” as meant by Tenn. Code § 47-18-103(2).

1123. Marriott advertised and sold “goods” or “services” in “consumer transaction[s],” as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

1124. Marriott advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And Marriott’s acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

1125. Marriott’s unfair and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Tennessee Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Tennessee Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Tennessee Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Tennessee Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Tennessee Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1126. Marriott intended to mislead Plaintiff and Tennessee Subclass members and induce them to rely on its misrepresentations and omissions.

1127. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1128. Had Marriott disclosed to Plaintiff and Tennessee Subclass members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiff's and Tennessee Subclass members' Personal Information as part of the services Marriott provided and

for which Plaintiff and Tennessee Subclass members paid without advising Plaintiff and Tennessee Subclass members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Tennessee Subclass members' Personal Information. Accordingly, Plaintiff and the Tennessee Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1129. Marriott had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiff and the Tennessee Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Tennessee Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Tennessee Subclass that contradicted these representations.

1130. Marriott's "unfair" acts and practices caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1131. The injury to consumers was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their

Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1132. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1133. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

1134. By misrepresenting and omitting material facts about its data security and failing to comply with its common law and statutory duties pertaining to data security (including its duties under the FTC Act), Marriott violated the following provisions of Tenn. Code § 47-18-104(b):

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve.

1135. Marriott acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiff and Tennessee Subclass members'

rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1136. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiff and Tennessee Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1137. Marriott's violations present a continuing risk to Plaintiff and Tennessee Subclass members as well as to the general public.

1138. Plaintiff and Tennessee Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

**CLAIMS ON BEHALF OF THE TEXAS SUBCLASS**

**COUNT 80**

**DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT,**

*Texas Bus. & Com. Code §§ 17.41, et seq.*

1139. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1140. Marriott is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

1141. Plaintiffs and the Texas Subclass members are “consumers,” as defined by Tex. Bus. & Com. Code § 17.45(4).

1142. Marriott advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

1143. Marriott engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised.

1144. Marriott’s false, misleading, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Texas Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas’s data security statute, Tex.

Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Texas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Texas Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

1145. Marriott intended to mislead Plaintiff and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

1146. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1147. Had Marriott disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business

and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services Marriott provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Personal Information. Accordingly, Plaintiff and the Texas Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1148. Marriott had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiffs and the Texas Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

1149. Marriott engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Marriott engaged in acts or practices which, to

consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

1150. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in Marriott's data security because this information was known exclusively by Marriott. Consumers also lacked the ability, experience, or capacity to secure the Personal Information in Marriott's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to Marriott's systems in order to evaluate its security controls. Marriott took advantage of its special skill and access to Personal Information to hide its inability to protect the security and confidentiality of Plaintiffs and Texas Subclass members' Personal Information.

1151. Marriott intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Marriott's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Marriott's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their Personal Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

1152. Marriott acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1153. As a direct and proximate result of Marriott's unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1154. Marriott's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

1155. Marriott's violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

1156. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; restitution; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

**CLAIMS ON BEHALF OF THE UTAH SUBCLASS**

**COUNT 81**

**UTAH CONSUMER SALES PRACTICES ACT,**

*Utah Code §§ 13-11-1, et seq.*

1157. The Utah Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Utah Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1158. Marriott is a “person,” as defined by Utah Code § 13-11-1(5).

1159. Marriott is a “supplier,” as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces “consumer transactions,” as defined by Utah Code § 13-11-1(2).

1160. Marriott engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Utah Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal

Information Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Utah Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Utah Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201.

1161. Marriott intended to mislead Plaintiff and Utah Subclass members and induce them to rely on its misrepresentations and omissions.

1162. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1163. Had Marriott disclosed to Plaintiff and Utah Subclass members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in

business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiff's and Utah Subclass members' Personal Information as part of the services Marriott provided and for which Plaintiff and Utah Subclass members paid without advising Plaintiff and Utah Subclass members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Utah Subclass members' Personal Information. Accordingly, Plaintiff and the Utah Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1164. Marriott had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiff and the Utah Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Utah Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Utah Subclass that contradicted these representations.

1165. Marriott intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

- a. indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not;
- b. indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;
- c. indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not;
- d. indicating that the subject of a consumer transaction will be supplied in greater quantity (e.g. more data security) than the supplier intends.

1166. Marriott engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. Marriott's acts and practices unjustly imposed hardship on Plaintiff and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity and cancelling and replacing passports; and lost value of their Personal Information. The deficiencies in Marriott's data security, and the material misrepresentations and omissions concerning those deficiencies, led to unfair surprise to Plaintiff and the Utah Subclass when the data breach occurred.

1167. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. Societal standards required Marriott, as one of the largest hotel conglomerates that collects, maintains, and compiles its customers' Personal Information, to adequately secure Personal Information in its possession. There is a substantial imbalance between

the obligations and rights of consumers, such as Plaintiff and the Utah Subclass, and Marriott, which has complete control over the Personal Information in its possession.

1168. Marriott's acts and practices were also procedurally unconscionable because consumers, including Plaintiff and the Utah Subclass, had no practicable option but to have their Personal Information stored in Marriott's systems if they wanted to utilize Marriott's services. Marriott exploited this imbalance in power, and the asymmetry of information about its data security, to profit by inadequately securing the Personal Information in its systems.

1169. As a direct and proximate result of Marriott's unconscionable and deceptive acts or practices, Plaintiffs and Utah Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1170. Marriott's violations present a continuing risk to Plaintiffs and Utah Subclass members as well as to the general public.

1171. Plaintiff and Utah Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of \$2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, et seq.; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE VERMONT SUBCLASS**

**COUNT 82**

**VERMONT CONSUMER FRAUD ACT,**

*Vt. Stat. Ann. Tit. 9, §§ 2451, et seq.*

1172. The Vermont Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Vermont Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1173. Plaintiff and Vermont Subclass members are “consumers,” as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

1174. Marriott’s conduct as alleged herein related to “goods” or “services” for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

1175. Marriott is a “seller,” as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

1176. Marriott advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

1177. Marriott engaged in unfair and deceptive acts or practices, in violation of Vt. Stat. tit. 9, § 2453(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Vermont Subclass members’ Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Vermont Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Vermont Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1178. Marriott intended to mislead Plaintiff and Vermont Subclass members and induce them to rely on its misrepresentations and omissions.

1179. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1180. Under the circumstances, consumers had a reasonable interpretation of Marriott's representations and omissions.

1181. Marriott had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiff and the Vermont Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Vermont Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Vermont Subclass that contradicted these representations.

1182. Marriott's acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1183. The injury to consumers was and is substantial because it was non-trivial and non-speculative; and involved a concrete monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1184. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of

consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1185. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

1186. Marriott is presumed, as a matter of law under Vt. Stat. Ann. tit. 9, § 2457, to have intentionally violated the Vermont Consumer Protection Act because it failed to sell goods or services in the manner and of the nature advertised or offered.

1187. Marriott acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Fraud Act, and recklessly disregarded Plaintiff and Vermont Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1188. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiffs and Vermont Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1189. Marriott's violations present a continuing risk to Plaintiffs and Vermont Subclass members as well as to the general public.

1190. Plaintiff and Vermont Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, actual damages, disgorgement of profits, treble damages, punitive/exemplary damages, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE VIRGIN ISLANDS SUBCLASS**

**COUNT 83**

**IDENTITY THEFT PREVENTION ACT,**

*V.I. Code Ann. tit. 14 §§ 2208, et seq.*

1191. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-295, as if fully alleged herein.

1192. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by V.I Code Ann. tit. 14 § 2201(a). Marriott also maintains computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to V.I Code Ann. tit. 14 §§ 2208(a) and (b).

1193. Virgin Islands Subclass members' Personal Information includes Personal Information covered by V.I Code Ann. tit. 14 § 2201(a).

1194. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Virgin Islands Subclass members, pursuant to V.I Code Ann. tit. 14 § 2208(b).

1195. Marriott is required to accurately notify Virgin Islands Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Marriott owns or licenses, in the most expedient time possible and without unreasonable delay under V.I Code Ann. tit. 14 § 2208(a).

1196. Because Marriott was aware of a security breach, Marriott had an obligation to disclose the data breach as mandated by V.I Code Ann. tit. 14 § 2208.

1197. As a direct and proximate result of Marriott's violations of V.I Code Ann. tit. 14 §§ 2208(a) and (b), Virgin Islands Subclass members suffered damages, as described above.

1198. Virgin Islands Subclass members seek relief under V.I Code Ann. tit. 14 §§ 2211(a) and (b), including actual damages, and injunctive relief.

**COUNT 84**

**VIRGIN ISLANDS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT,**

*Virgin Islands Code tit. 12A, §§ 301, et seq.*

1199. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-295, as if fully alleged herein.

1200. Marriott is a "person," as defined by V.I. Code tit. 12A, § 303(h).

1201. Plaintiff and Virgin Islands Subclass members are "consumers," as defined by V.I. Code tit. 12A, § 303(d).

1202. Marriott advertised, offered, or sold goods or services in the Virgin Islands and engaged in trade or commerce directly or indirectly affecting the people of the Virgin Islands.

1203. Marriott engaged in unfair and deceptive acts and practices, in violation of V.I. Code tit. 12A, § 304, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virgin Islands Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virgin Islands Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virgin Islands Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1204. Marriott's acts and practices were "unfair" under V.I. Code tit. 12A, § 304 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1205. The injury to consumers from Marriott's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk

to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1206. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1207. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

1208. Marriott's acts and practices were "deceptive" under V.I. Code tit. 12A, §§ 303 & 304 because Marriott made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

1209. Marriott intended to mislead Plaintiff and Virgin Island Subclass members and induce them to rely on its misrepresentations and omissions.

1210. Marriott's representations and omissions were material because they were likely to unfairly influence or deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1211. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiff and the Virgin Islands Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for

Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virgin Islands Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

1212. Marriott acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiff and Virgin Islands Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate. Marriott intentionally hid the inadequacies in its data security, callously disregarding the rights of consumers.

1213. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent

activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1214. Marriott's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

1215. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory, consequential, treble, punitive, and equitable damages under V.I. Code tit. 12A, § 331; injunctive relief; and reasonable attorneys' fees and costs.

### **COUNT 85**

#### **VIRGIN ISLANDS CONSUMER PROTECTION LAW.**

*V.I. Code tit. 12A, §§101, et seq.*

1216. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-295, as if fully alleged herein.

1217. Marriott is a "merchant," as defined by V.I. Code tit. 12A, § 102(e).

1218. Plaintiff and Virgin Islands Subclass members are "consumers," as defined by V.I. Code tit. 12A, § 102(d).

1219. Marriott sells and offers for sale "consumer goods" and "consumer services," as defined by V.I. Code tit. 12A, § 102(c).

1220. Marriott engaged in deceptive acts and practices, in violation of V.I. Code tit. 12A, § 101, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virgin Islands Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virgin Islands Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virgin Islands Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1221. Marriott's acts and practices were "deceptive trade practices" under V.I. Code tit. 12A, § 102(a) because Marriott:

- a. Represented that goods or services have sponsorship, approval, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have; or that goods or services are of particular standard, quality, grade, style or model, if they are of another;
- b. Used exaggeration, innuendo or ambiguity as to a material fact or failure to state a material fact if such use deceives or tends to deceive;
- c. Offered goods or services with intent not to sell them as offered;
- d. Stated that a consumer transaction involves consumer rights, remedies or obligations that it does not involve.

1222. Marriott's acts and practices were also "deceptive" under V.I. Code tit. 12A, § 101 because Marriott made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

1223. Marriott intended to mislead Plaintiff and Virgin Islands Subclass members and induce them to rely on its misrepresentations and omissions.

1224. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1225. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiff and the Virgin Islands Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship

between consumers—including Plaintiff and the Virgin Islands Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

1226. Marriott acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Protection Law, and recklessly disregarded Plaintiff and Virgin Island Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1227. As a direct and proximate result of Marriott's deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1228. Marriott's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

1229. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory relief; injunctive relief; the greater of actual damages or \$500 per violation; compensatory, consequential, treble, and punitive damages; restitution; disgorgement; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS**

**COUNT 86**

**VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT,**

*Va. Code Ann. §§ 18.2-186.6, et seq.*

1230. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1231. Marriott is required to accurately notify Plaintiff and Virginia Subclass members following discovery or notification of a breach of its data security system if unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

1232. Marriott is an entity that owns or licenses computerized data that includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(B).

1233. Plaintiff's and Virginia Subclass members' Personal Information includes Personal Information as covered under Va. Code Ann. § 18.2-186.6(A).

1234. Because Marriott discovered a breach of its security system in which unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in

identify theft or another fraud, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

1235. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Va. Code Ann. § 18.2-186.6(B).

1236. As a direct and proximate result of Marriott's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass members suffered damages, as described above.

1237. Plaintiff and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

### **COUNT 87**

#### **VIRGINIA CONSUMER PROTECTION ACT,**

*Va. Code Ann. §§ 59.1-196, et seq.*

1238. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1239. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

1240. Marriott is a "person" as defined by Va. Code Ann. § 59.1-198.

1241. Marriott is a "supplier," as defined by Va. Code Ann. § 59.1-198.

1242. Marriott engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Marriott advertised, offered, or sold goods or services used primarily for personal, family or household purposes; or relating to an individual's finding or obtaining employment.

1243. Marriott engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virginia Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virginia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virginia Subclass members' Personal Information; and

- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1244. Marriott intended to mislead Plaintiff and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1245. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Virginia Subclass members, about the adequacy of Marriott's computer and data security and the quality of the Marriott brand.

1246. Had Marriott disclosed to Plaintiff and Virginia Subclass members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiff's and Virginia Subclass members' Personal Information as part of the services Marriott provided and for which Plaintiff and Virginia Subclass members paid without advising Plaintiff and Virginia Subclass members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Virginia Subclass members' Personal Information. Accordingly, Plaintiff and the Virginia Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1247. In Marriott had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virginia Subclass—and Marriott, because consumers are unable to fully protect

their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virginia Subclass that contradicted these representations.

1248. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

- a. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;
- b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and
- c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

1249. Marriott acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish Marriott for its wrongdoing, and warn or deter others from engaging in similar conduct.

1250. As a direct and proximate result of Marriott's deceptive acts or practices, Plaintiffs and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable

losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1251. Marriott's violations present a continuing risk to Plaintiffs and Virginia Subclass members as well as to the general public.

1252. Plaintiff and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of \$1,000 per violation if the conduct is found to be willful or, in the alternative, \$500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS**

**COUNT 88**

**WASHINGTON DATA BREACH NOTICE ACT,**

*Wash. Rev. Code §§ 19.255.010, et seq.*

1253. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1254. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Wash. Rev. Code § 19.255.010(1).

1255. Plaintiff's and Washington Subclass members' Personal Information includes Personal Information as covered under Wash. Rev. Code § 19.255.010(5).

1256. Marriott is required to accurately notify Plaintiff and Washington Subclass members following discovery or notification of the breach of its data security system if Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

1257. Because Marriott discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

1258. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Wash. Rev. Code § 19.255.010(1).

1259. As a direct and proximate result of Marriott's violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Washington Subclass members suffered damages, as described above.

1260. Plaintiff and Washington Subclass members seek relief under Wash. Rev. Code §§ 19.255.010(13)(a) and 19.255.010(13)(b), including actual damages and injunctive relief.

### **COUNT 89**

#### **WASHINGTON CONSUMER PROTECTION ACT,**

*Wash. Rev. Code Ann. §§ 19.86.020, et seq.*

1261. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1262. Marriott is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1263. Marriott advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

1264. Marriott engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Washington Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Washington Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Washington Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1265. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1266. Marriott acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1267. Marriott's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

1268. As a direct and proximate result of Marriott's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would

not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1269. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE WEST VIRGINIA SUBCLASS**

**COUNT 90**

**WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT,**

*W. Va. Code §§46A-6-101, et seq.*

1270. The West Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the West Virginia Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1271. Plaintiff and West Virginia Subclass members are "consumers," as defined by W. Va. Code § 46A-6-102(2).

1272. Marriott engaged in "consumer transactions," as defined by W. Va. Code § 46A-6-102(2).

1273. Marriott advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code § 46A-6-102(6).

1274. Plaintiff sent a demand for relief on behalf of the West Virginia Subclass pursuant to W. Va. Code § 46A-6-106(c) on January 8, 2019. Marriott has not cured its unfair and deceptive acts and practices.

1275. Marriott engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code § 46A-6-104, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and West Virginia Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and West Virginia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and West Virginia Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1276. Marriott's unfair and deceptive acts and practices also violated W. Va. Code § 46A-6-102(7), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;
- e. Using deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of goods or services, whether or not any person has in fact been misled, deceived or damaged thereby;
- f. Advertising, displaying, publishing, distributing, or causing to be advertised, displayed, published, or distributed in any manner, statements and representations with regard to

the sale of goods or the extension of consumer credit, which are false, misleading or deceptive or which omit to state material information which is necessary to make the statements therein not false, misleading or deceptive;

1277. Marriott's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code § 46A-6-101.

1278. Marriott's acts and practices were additionally "unfair" under W. Va. Code § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1279. The injury to consumers from Marriott's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1280. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1281. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

1282. Marriott's acts and practices were additionally "deceptive" under W. Va. Code § 46A-6-104 because Marriott made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiff and West Virginia Subclass members.

1283. Marriott intended to mislead Plaintiff and West Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1284. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1285. Had Marriott disclosed to Plaintiff and West Virginia Subclass members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott received, maintained, and compiled Plaintiff's and West Virginia Subclass members' Personal Information as part of the services Marriott provided and for which Plaintiff and West Virginia Subclass members paid without advising Plaintiff and West Virginia Subclass members that Marriott's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and West Virginia Subclass members' Personal Information. Accordingly, Plaintiff and the West Virginia Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1286. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiff and the West Virginia Subclass members reposed a trust and

confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the West Virginia Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the West Virginia Subclass that contradicted these representations.

1287. Marriott's omissions were legally presumed to be equivalent to active misrepresentations because Marriott intentionally prevented Plaintiff and West Virginia Subclass members from discovering the truth regarding Marriott's inadequate data security.

1288. Marriott acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiff and West Virginia Subclass members' rights. Marriott's unfair and deceptive acts and practices were likely to cause serious harm. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1289. As a direct and proximate result of Marriott's unfair and deceptive acts or practices and Plaintiff and West Virginia Subclass members' purchase of goods or services, Plaintiff and West Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services

or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1290. Marriott's violations present a continuing risk to Plaintiff and West Virginia Subclass members as well as to the general public.

1291. Plaintiff and West Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$200 per violation under W. Va. Code § 46A-6-106(a); restitution, injunctive and other equitable relief; punitive damages, and reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS**

#### **COUNT 91**

#### **NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION.**

*Wis. Stat. §§ 134.98(2), et seq.*

1292. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1293. Marriott is a business that maintains or licenses Personal Information as defined by Wis. Stat. § 134.98(2).

1294. Plaintiff's and Wisconsin Subclass members' Personal Information includes Personal Information as covered under Wis. Stat. § 134.98(1)(b).

1295. Marriott is required to accurately notify Plaintiff and Wisconsin Subclass members if it knows that Personal Information in its possession has been acquired by a person whom it has

not authorized to acquire the Personal Information within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

1296. Because Marriott knew that Personal Information in its possession had been acquired by a person whom it has not authorized to acquire the Personal Information, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

1297. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Wis. Stat. § 134.98(2).

1298. As a direct and proximate result of Marriott's violations of Wis. Stat. § 134.98(3)(a), Plaintiff and Wisconsin Subclass members suffered damages, as described above.

1299. Plaintiff and Wisconsin Subclass members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

## **COUNT 92**

### **WISCONSIN DECEPTIVE TRADE PRACTICES ACT,**

*Wis. Stat. § 100.18*

1300. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1301. Marriott is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

1302. Plaintiff and Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

1303. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Marriott to members of the public for sale, use, or distribution, Marriott

made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

1304. Marriott also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

1305. Marriott's deceptive acts, practices, plans, and schemes include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Wisconsin Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Wisconsin Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Wisconsin Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1306. Marriott intended to mislead Plaintiff and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

1307. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1308. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiff and the Wisconsin Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Wisconsin Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

1309. Marriott's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

1310. Marriott acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass members' rights. Marriott's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

1311. As a direct and proximate result of Marriott's deceptive acts or practices, Plaintiff and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Marriott as they would not have paid Marriott for goods and services or would have paid less for such goods and services but for Marriott's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1312. Marriott had an ongoing duty to all Marriott customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

1313. Plaintiff and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

**CLAIMS ON BEHALF OF THE WYOMING SUBCLASS**

**COUNT 93**

**COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS.**

*Wyo. Stat. Ann. §§ 40-12-502(a), et seq.*

1314. The Wyoming Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wyoming Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1315. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Wyo. Stat. Ann. § 40-12-502(a).

1316. Plaintiff's and Wyoming Subclass members' Personal Information includes Personal Information as covered under Wyo. Stat. Ann. § 40-12-502(a).

1317. Marriott is required to accurately notify Plaintiff and Wyoming Subclass members when it becomes aware of a breach of its data security system if the misuse of personal identifying information has occurred or is reasonably likely to occur, in the most expedient time possible and without unreasonable delay under Wyo. Stat. Ann. § 40-12-502(a).

1318. Because Marriott was aware of a breach of its data security system in which the misuse of personal identifying information has occurred or is reasonably likely to occur, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Wyo. Stat. Ann. § 40-12-502(a).

1319. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Wyo. Stat. Ann. § 40-12-502(a).

1320. As a direct and proximate result of Marriott's violations of Wyo. Stat. Ann. § 40-12-502(a), Plaintiff and Wyoming Subclass members suffered damages, as described above.

1321. Plaintiff and Marriott Subclass members seek relief under Wyo. Stat. Ann. § 40-12-502(f), including actual damages and equitable relief.

#### **COUNT 94**

#### **WYOMING CONSUMER PROTECTION ACT,**

*Wyo. Stat. Ann. §§ 40-12-101, et seq.*

1322. The Wyoming Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wyoming Subclass, repeats and alleges Paragraphs 1-295, as if fully alleged herein.

1323. Marriott is a "person" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(i).

1324. Marriott's goods and services are "merchandise" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(vi).

1325. Marriott engages in "consumer transactions" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(ii).

1326. Marriott has "advertised" its goods and services within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(v).

1327. Plaintiff sent a demand for relief on behalf of the Wyoming Subclass pursuant to Wyo. Stat. Ann. § 40-12-109 on January 8, 2019. Marriott has not cured the deceptive trade practices described below.

1328. Marriott knowingly engaged in unfair and deceptive trade practices in the course of its business and in connection with consumer transactions, including by:

- a. Failing to implement and maintain reasonable security measures to protect Plaintiff and Wyoming Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Failing to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents;
- c. Failing to comply with common law and statutory duties pertaining to the security of Plaintiff and Wyoming Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- d. Misrepresenting that it would implement and maintain reasonable security measures to protect Plaintiff and Wyoming Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Plaintiff and Wyoming Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Wyoming Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of Plaintiff and Wyoming Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1329. Through the above-described conduct, Marriott violated Wyo. Stat. Ann. § 40-12-105(a) by:

- a. Knowingly representing that goods or services have sponsorship, approval, accessories or uses they do not have;
- b. Knowingly representing that goods or services are of a particular standard or grade, if they are not;
- c. Knowingly representing that goods or services have been supplied in accordance with a previous representation, if they have not;
- d. Knowingly advertising goods or services with intent not to sell them as advertised; and
- e. Knowingly engaging in unfair or deceptive acts or practices.

1330. Marriott intentionally made the above-described representations and omissions of material fact with knowledge of their falsity or reckless disregard of the truth. Marriott knew or should have known that its computer systems and data security practices were inadequate to protect Plaintiff and Wyoming Subclass members' Personal Information and that a data breach or theft was highly likely to occur. Marriott's past data breaches and breaches within the hospitality industry, among other things, did or should have put it on notice that its security was inadequate. In making its representations and omissions, Marriott intended to mislead Plaintiff and Wyoming Subclass members and cause them to act or elect not to act based on these representations and omissions. Marriott knew or should have known that its conduct violated Wyo. Stat. § 40-12-105.

1331. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Wyoming Subclass members, about the adequacy of Marriott's computer and data security and the quality of the Marriott brand.

1332. Plaintiff and Wyoming Subclass members were ignorant of the falsity of Marriott's representations and omissions, and relied upon these representations and omissions in choosing to act or not act.

1333. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. This duty arose because Plaintiff and the Wyoming Subclass members reposed a trust and confidence in Marriott when they provided their Personal Information to Marriott in exchange for Marriott's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Wyoming Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its general duty to exercise reasonable care and its knowledge that Plaintiff and Wyoming Subclass members might justifiably be induced, by Marriott's omissions, to act or refrain from acting in a business transaction. Additionally, Marriott's had a duty to disclose inadequacies in its data security because such facts were basic to the transactions in question; Marriott knew Plaintiff and Wyoming Subclass members were mistaken as to these facts and would enter transactions as a result; and based on objective circumstances, Plaintiff and Wyoming Subclass members would reasonably expect a disclosure of those facts. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wyoming Subclass that contradicted these representations.

1334. As described above, Marriott's statements and omissions were likely to deceive a reasonable consumer because consumers provided their Personal Information to Marriott in exchange for Marriott's services and because Marriott kept the inadequate state of its security

controls secret from the public. In light of its direct relationship with its customers, Marriott's statements concerning data security constitute representations that its security was, at minimum, reasonable.

1335. Marriott's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1336. The injury to consumers from Marriott's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1337. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1338. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

1339. As a direct and proximate result of Marriott's uncured unfair and deceptive acts or practices, Plaintiff and Wyoming Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and/or non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial

accounts for fraudulent activity and cancelling and replacing passports; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1340. Plaintiff and Wyoming Subclass members seek relief pursuant to Wyo. Stat. Ann. § 40-12-108, including damages and reasonable attorneys' fees.

**CLAIMS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ACCENTURE**

**COUNT 95**

**NEGLIGENCE**

**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

1341. Plaintiffs repeat and allege Paragraphs 1-295, as if fully alleged herein.

1342. Accenture owed a duty to Plaintiffs and class members to exercise reasonable care in securing and safeguarding and protecting their Personal Information in Starwood's databases from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing the security systems of Starwood and Marriott to ensure that Plaintiffs' and class members' Personal Information in Starwood's and Marriott's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

1343. Accenture had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of Accenture's inadequate security practices. Accenture knew that its failure to secure its clients' networks or detect and identify IT security threats could result in the exposure of Plaintiffs' and

class members' Personal Information and cause significant harm, which Accenture acknowledged in its own public filings.

1344. Accenture's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Accenture. Various FTC publications and data security breach orders further form the basis of Accenture's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

1345. Accenture also had a duty to safeguard the Personal Information of Plaintiffs and class members because of state laws and statutes that require Accenture to reasonably safeguard Personal Information, as detailed herein.

1346. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1347. Accenture breached the duties it owed to Plaintiffs and class members described above and thus was negligent. Accenture breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiffs and class members; (b) detect and identify known and obvious security threats; (c) detect the breach while it was ongoing; and (d) maintain its clients' security systems consistent with industry standards.

1348. Accenture's wrongful and negligent breach of its duties owed to Plaintiffs and class members caused their Personal Information to be compromised.

1349. As a direct and proximate result of Accenture's negligence, Plaintiffs and class members have been injured as described herein, and are entitled to damages in an amount to be proven at trial. Plaintiffs and class members injuries include:

- a. purchasing goods and services they would not have otherwise paid for and/or paying more for goods and services than they otherwise would have paid, had they known the truth about Accenture's substandard data security practices;
- b. losing the inherent value of their Personal Information;
- c. losing the value of the explicit and implicit promises of data security;
- d. identity theft and fraud resulting from the theft of their Personal Information;
- e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

- g. costs associated with replacing passports or addressing passport-related fraud;
- h. loss of value of reward points accumulated through the purchase of goods or services;
- i. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- j. lowered credit scores resulting from credit inquiries following fraudulent activities;
- k. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and
- l. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

**COUNT 96**

**NEGLIGENCE PER SE**

**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

1350. Plaintiffs repeat and allege Paragraphs 1-295, as if fully alleged herein.

1351. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair act or practice by companies such as Marriott of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Marriott’s duty.

1352. Accenture violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry standards. Accenture’s conduct was particularly unreasonable given the nature and amount of Personal Information it knew was stored on Starwood’s database, its obligations to safeguard that information knowing the inherent risks of storing such information, and the foreseeable consequences of a data breach on Starwood’s systems.

1353. Accenture’s violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

1354. Nationwide Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

1355. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

1356. As a direct and proximate result of Accenture’s negligence, Plaintiffs and Class members have been injured as described herein, and are entitled to damages in an amount to be proven at trial.

### **REQUEST FOR RELIEF**

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;
2. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. That the Court award Plaintiffs and Class and Subclass members compensatory, consequential, and general damages in an amount to be determined at trial;
4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;
5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;
6. That Plaintiffs be granted the declaratory relief sought herein;
7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
8. That the Court award pre- and post-judgment interest at the maximum legal rate; and
9. That the Court grant all such other relief as it deems just and proper.

### **DEMAND FOR JURY TRIAL**

Plaintiffs demand a jury trial on all claims so triable.

Dated: August 26, 2019

Respectfully submitted,

/s/ Amy E. Keller

Amy E. Keller (D. Md. Bar No. 20816)  
**DiCELLO LEVITT GUTZLER LLC**  
Ten North Dearborn Street, Eleventh Floor  
Chicago, Illinois 60602  
Tel. 312-214-7900  
[akeller@dlcfirm.com](mailto:akeller@dlcfirm.com)

/s/ James J. Pizzirusso

James J. Pizzirusso (D. Md. Bar No. 20817)  
**HAUSFELD LLP**  
1700 K Street NW Suite 650  
Washington, D.C. 20006  
Tel. 202-540-7200  
[jpizzirusso@hausfeld.com](mailto:jpizzirusso@hausfeld.com)

/s/ Andrew N. Friedman

Andrew N. Friedman (D. Md. Bar No. 14421)  
**COHEN MILSTEIN SELLERS & TOLL  
PLLC**  
1100 New York Avenue, NW, Suite 500  
Washington, D.C. 20005  
Tel. 202-408-4600  
[afriedman@cohenmilstein.com](mailto:afriedman@cohenmilstein.com)

*Consumer Plaintiffs' Co-lead Counsel*

Norman E. Siegel  
**STUEVE SIEGEL HANSON LLP**  
460 Nichols Road, Suite 200  
Kansas City, Missouri 64112  
Tel: 816-714-7100  
[siegel@stuevesiegel.com](mailto:siegel@stuevesiegel.com)

MaryBeth V. Gibson  
**THE FINLEY FIRM, P.C.**  
3535 Piedmont Road, Bldg. 14, Suite 230  
Atlanta, GA 30305  
Tel: 404-320-9979  
[mgibson@thefinleyfirm.com](mailto:mgibson@thefinleyfirm.com)

Ariana J. Tadler  
**TADLER LAW LLP**  
One Penn Plaza, 36th Floor  
New York, NY 10119  
Tel: 212-946-9300  
[atadler@tadlerlaw.com](mailto:atadler@tadlerlaw.com)

Jason Lichtman  
**LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLP**  
250 Hudson Street, 8th Floor  
New York, NY 10013  
Tel: 212-355-9500  
[jlichtman@lchb.com](mailto:jlichtman@lchb.com)

Daniel Robinson  
**ROBINSON CALCAGNIE, INC.**  
19 Corporate Plaza Drive  
Newport Beach, CA 92660  
Tel: 949-720-1288  
[drobinson@robinsonfirm.com](mailto:drobinson@robinsonfirm.com)

Megan Jones  
**HAUSFELD LLP**  
600 Montgomery Street, Suite 3200  
San Francisco, CA 94111  
Tel: 415-633-1908  
[mjones@hausfeld.com](mailto:mjones@hausfeld.com)

Timothy Maloney  
**JOSEPH GREENWALD & LAAKE, P.A.**  
6404 Ivy Lane, Suite 400  
Greenbelt, MD 20770  
Tel: 301-220-2200  
[tmaloney@jgllaw.com](mailto:tmaloney@jgllaw.com)

Gary F. Lynch  
**CARLSON LYNCH LLP**  
1133 Penn Avenue, 5th Floor  
Pittsburgh, PA 15222  
Tel: 412-322-9243  
[glynch@carlsonlynch.com](mailto:glynch@carlsonlynch.com)

*Consumer Plaintiffs' Steering Committee*

Veronica Nannis  
**JOSEPH GREENWALD & LAAKE, P.A.**  
6404 Ivy Lane, Suite 400  
Greenbelt, MD 20770  
Tel: 301-220-2200  
[vnannis@jgllaw.com](mailto:vnannis@jgllaw.com)

James Ulwick  
**KRAMON & GRAHAM PA**  
1 South Street, Suite 2600  
Baltimore, MD 21202  
Tel: 410-347-7426  
[julwick@kg-law.com](mailto:julwick@kg-law.com)

*Consumer Plaintiffs' Liaison Counsel*

**CERTIFICATE OF SERVICE**

I, Veronica Nannis, Co-Liaison Counsel for the Consumer Plaintiffs, hereby certify that on August 26, 2019, I served the above and foregoing Consolidated Consumer Class Action Complaint on all counsel of record by filing it electronically with the Clerk of the Court using the CM/ECF filing system.

/s/ Veronica Nannis